RECORD AND BRIEF

16-402

No. _____

FILED
SEP 26 2016
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Steven R. Shapiro
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226

QUESTION PRESENTED

In this case, as in thousands of cases each year, the government sought and obtained the historical cell phone location data of a private individual pursuant to a disclosure order under the Stored Communications Act (SCA) rather than by securing a warrant. Under the SCA, a disclosure order does not require a finding of probable cause. Instead, the SCA authorizes the issuance of a disclosure order whenever the government "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

As a result, the district court never made a probable cause finding before ordering Petitioner's service provider to disclose months' worth of Petitioner's cell phone location records. A divided panel of the Sixth Circuit held that there is no reasonable expectation of privacy in these location records, relying in large part on four-decade-old decisions of this Court.

The Question Presented is:

Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment.

PARTIES TO THE PROCEEDINGS

In addition to the parties named in the caption, Timothy Michael Sanders was a defendant-appellant below, and was represented by separate counsel.

TABLE OF CONTENTS

QUESTION PRESENTED i

PARTIES TO THE PROCEEDINGS ii

TABLE OF AUTHORITIES vi

PETITION FOR A WRIT OF CERTIORARI 1

OPINIONS BELOW 1

JURISDICTION 1

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS 1

STATEMENT OF THE CASE 3

REASONS FOR GRANTING THE WRIT 10

I. THIS CASE PRESENTS AN IMPORTANT AND RECURRING QUESTION ON THE SCOPE OF CONSTITUTIONAL PRIVACY RIGHTS IN THE DIGITAL AGE 10

A. The Lower Courts Have Expressly and Repeatedly Sought This Court's Guidance in Addressing the Question Presented. ... 10

B. This Court's Recent Decisions Have Properly Recognized a Need to Reexamine Traditional Understandings of Privacy in the Digital Age 16

C. The Volume and Frequency of Warrantless Law Enforcement Requests for CSLI Highlights the Importance of the Question Presented. 18

II. FEDERAL COURTS OF APPEALS AND STATE HIGH COURTS ARE DIVIDED. 21

A. The Circuits Are Split Over Whether the Third-Party Doctrine Eliminates People's Reasonable Expectation of Privacy in Their Historical CSLI. 21

B. The Circuits Are Split Over Whether There is a Reasonable Expectation of Privacy in Longer-Term Location Information Collected by Electronic Means. 24

III. THE SIXTH CIRCUIT ERRED IN HOLDING THAT THE CONDUCT HERE WAS NOT A SEARCH 26

A. The Sixth Circuit Erred in Holding That There Is No Reasonable Expectation of Privacy in Historical CSLI. 26

B. The Sixth Circuit Erred In Deferring to Congress's 30-Year-Old Legislative Scheme. 32

CONCLUSION 35

APPENDIX 1a

Opinion, United States Court of Appeals for the Sixth Circuit (April 13, 2016) 1a

Order, United States Court of Appeals for the Sixth Circuit (June 29, 2016) 33a

Opinion & Order, United States District Court, Eastern District Of Michigan, Southern Division (Dec. 6, 2013) 34a

Application, United States District Court, Eastern District Of Michigan, Southern Division (May 2, 2011) 49a

Order, United States District Court, Eastern District of Michigan, Southern Division (May 2, 2011) 56a

Application, United States District Court, Eastern District of Michigan, Southern Division (June 7, 2011) 62a

Order, United States District Court, Eastern District of Michigan, Southern Division (June 7, 2011) 69a

Government Trial Exhibit 57, Federal Bureau Of Investigation Cellular Analysis (Nov. 5, 2013) ... 74a

TABLE OF AUTHORITIES

CASES

Bond v. United States, 529 U.S. 334 (2000) 27

Chapman v. United States, 365 U.S. 610 (1961) 27

Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) 23

Ferguson v. City of Charleston, 532 U.S. 67 (2001). 27

Florida v. Jardines, 133 S. Ct. 1409 (2013) 26

In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011 (N.D. Cal. 2015), *appeal dismissed*, No. 15-16760 (9th Cir. Feb. 5, 2016) 29

In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) 14, 22, 34

In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010) 14, 22, 23, 28

Katz v. United States, 389 U.S. 347 (1967) .....*passim*

Kyllo v. United States, 533 U.S. 27 (2001) 17, 26, 28, 30

Minnesota v. Olson, 495 U.S. 91 (1990) 27

New York v. Belton, 453 U.S. 454 (1981) 16

Riley v. California, 134 S. Ct. 2473 (2014) .....*passim*

Smith v. Maryland, 442 U.S. 735 (1979) .....*passim*

State v. Earls, 70 A.3d 630 (N.J. 2013) 24

Stoner v. California, 376 U.S. 483 (1964) 27

Tracey v. State, 152 So. 3d 504 (Fla. 2014) 24, 32

United States v. Davis, 754 F.3d 1205 (11th Cir. 2014), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015) 14, 29

United States v. Davis, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015) .....*passim*

United States v. Garcia, 474 F.3d 994 (7th Cir. 2007) 25

United States v. Graham, 796 F.3d 332 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016) 14

United States v. Graham, 824 F.3d 421 (4th Cir. 2016) .....*passim*

United States v. Guerrero, 768 F.3d 351 (5th Cir. 2014) 22

United States v. Jacobsen, 466 U.S. 109 (1984)..... 27

United States v. Jones, 132 S. Ct. 945 (2012) ...*passim*

United States v. Karo, 468 U.S. 705 (1984) 29

United States v. Marquez, 605 F.3d 604 (8th Cir. 2010) 25

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) 24, 25

United States v. Miller, 425 U.S. 435 (1976) ....*passim*

United States v. Pineda-Moreno, 617 F.3d 1120 (9th Cir. 2010) 20, 25

United States v. Skinner, 690 F.3d 772 (6th Cir. 2012) 8

United States v. Knotts, 460 U.S. 276 (1983)..... 20

Zanders v. State, No. 15A01–1509-CR–1519, __ N.E.3d __, 2016 WL 4140998 (Ind. Ct. App. Aug. 4, 2016), *pet. to transfer jurisdiction to Indiana Supreme Court filed* (Sept. 6, 2016) 14, 23

CONSTITUTION & STATUTES

U.S. Const. amend. IV ..... *passim*

Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 207, 108 Stat. 4279 (1994) 33

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848 33

Hobbs Act, 18 U.S.C. § 1951(a) 9

Stored Communications Act, 18 U.S.C. § 2703 *et seq.* ..... *passim*

18 U.S.C. § 2703(c)(1)(A) 34

18 U.S.C. § 2703(d) ..... i, 3, 22

18 U.S.C. § 924(c) 9

28 U.S.C. § 1254(1) 1

725 Ill. Comp. Stat. 168/10 24

Colo. Rev. Stat. § 16-3-303.5(2) 23

Ind. Code 35-33-5-12 24

Md. Code Ann. Crim. Proc. § 1-203.1(b) 24

Me. Rev. Stat. tit. 16, § 648 23

Minn. Stat. §§ 626A.28(3)(d), 626A.42(2) 23

Mont. Code Ann. § 46-5-110(1)(a) 23

N.H. Rev. Stat. Ann. § 644-A:2 23

Utah Code Ann. § 77-23c-102(1)(a) 23

Va. Code Ann. § 19.2-70.3(C) 24

Vt. Stat. Ann. tit. 13, § 8102(b) 23

OTHER AUTHORITIES

American Civil Liberties Union, Cell Phone Location Tracking Public Records Request (Mar. 25, 2013) 20

Andrea Meyer, *30th Anniversary of the First Commercial Cell Phone Call*, Verizon (Oct. 11, 2013) 33, 34

Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Syss. Design & Implementation 20 (2011) 31

AT&T, *Transparency Report* (2015) 19

Background on CTIA's Wireless Industry Survey, CTIA-The Wireless Association (2014) 33

CTIA – The Wireless Association, *Annual Wireless Industry Survey* (2014) 7, 18, 33

Daniel Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087 (2002) 15

Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014) 32

Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 Stan. L. Rev. 119 (2002) 15

Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January-June 2014* (Dec. 2014) 18

T-Mobile, *Transparency Report for 2013 & 2014* (2015) 19

Will Baude, *Further Thoughts on the Precedential Status of Decisions Affirmed on Alternate Grounds*, The Volokh Conspiracy (Dec. 3, 2013, 7:27 PM), http://volokh.com/2013/12/03/thoughts-precedential-status-decisions-affirmed-alternate-grounds/ 25

PETITION FOR A WRIT OF CERTIORARI

Petitioner Timothy Carpenter respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Sixth Circuit.

OPINIONS BELOW

The opinion of the Sixth Circuit (Pet. App. 1a–32a) is reported at 819 F.3d 880. The district court opinion (Pet. App. 34a–48a) is unpublished, but is available at 2013 WL 6385838.

JURISDICTION

The Sixth Circuit issued its opinion on April 13, 2016, and denied rehearing en banc on June 29, 2016. (Pet. App. 33a). This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment to the U.S. Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Stored Communications Act, 18 U.S.C. § 2703, provides in relevant part:

> **(c) Records concerning electronic communication service or remote computing service.**--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
>
> > **(A)** obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; [or]
> >
> > **(B)** obtains a court order for such disclosure under subsection (d) of this section; * * *
>
> **(d) Requirements for court order.**--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other

> information sought, are relevant and material to an ongoing criminal investigation. * * *

STATEMENT OF THE CASE

This case presents the pressing question of whether the Fourth Amendment protects against the government's warrantless acquisition of cell phone records revealing an individual's location and movements over extended periods of time.

1. During the course of an investigation into a series of armed robberies that occurred in southeastern Michigan and northwestern Ohio in 2010 and 2011, an Assistant United States Attorney submitted to different magistrate judges three applications for orders to access more than five months of historical cell phone location records for Petitioner Timothy Carpenter and several other suspects. Pet. App. 3a, 49a–55a, 62a–68a. The applications, which were unsworn, did not seek warrants based on probable cause, but rather orders under the Stored Communications Act, 18 U.S.C. § 2703(d). Such an order may issue when the government "offers specific and articulable facts showing that there are reasonable grounds to believe that" the records sought "are relevant and material to an ongoing criminal investigation." *Id.*

The applications sought "[a]ll subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target telephones from December 1, 2010 to present[,]" as well as "cell site information for the target telephones at call origination and at call termination

for incoming and outgoing calls[.]" Pet. App. 4a (alterations in original); *see also id.* at 52a. The applications stated that "a cooperating defendant was interviewed about his involvement in [several] armed robberies and admitted he had a role in eight different robberies that started in December of 2010 and lasted through March of 2011 at Radio Shack and T-Mobile stores in Michigan and Ohio." Pet. App. 53a. The applications further asserted that "the requested telecommunications records should yield information that is relevant and material to corroborate surveillance information and may identify potential witnesses and/or targets. The requested information will . . . provide evidence that . . . Timothy Carpenter and other known and unknown individuals are violating provisions of Title 18, United States Code, §1951." Pet. App. 54a. Rather than restricting the request to only the days on which the robberies occurred, however, the primary application at issue here, which was submitted on May 2, 2011, sought records "from December 1, 2010 to present." Pet. App. 52a. That constituted a request for 152 days of data.

Orders granting the applications were issued on May 2 and June 7, 2011. Pet. App. 56a–61a, 69a–73a. The May 2 order directed MetroPCS, Carpenter's cellular service provider, to "provide the locations of cell/site sector (physical addresses) for the target telephones at call origination and at call termination for incoming and outgoing calls" from "December 1, 2010 to present." Pet. App. 59a–60a. MetroPCS complied, providing 186 pages of

Carpenter's cell phone records to the government.[1] Those records show each of Carpenter's incoming and outgoing calls over the course of 127 days,[2] along with the cell tower ("cell site") and directional sector of the tower that Carpenter's phone connected to at the start and end of most of the calls.[3] Pet. App. 5a–7a.

A separate order, issued on June 7, 2011, directed Sprint to produce cell site location information for Carpenter's phone while it was "roaming on Sprint's cellular tower network" from March 1 to March 7, 2011. Pet. App. 72a. "Metro PCS does not have coverage in the Warren, Ohio area," where one of the charged robberies took place, and

---

[1] A sample page from Carpenter's records was entered into evidence at trial. Defendant's Trial Ex. 3. The full records were provided by the government to the defense in pre-trial discovery and were discussed by a prosecution's witness at trial, Trial Tr. 46, Dec. 13, 2013, ECF No. 332, but were not made part of the record before the district court. They were filed as an appendix to the Amicus Brief of the American Civil Liberties Union, et al., at the Sixth Circuit. *See* Doc. No. 33-1 The parties stipulated at trial that the cell site location records from "Metro PCS and Sprint utilized by [government witness] FBI Special Agent Christopher Hess to formulate his analysis and opinion are authentic and accurate business records of these companies." Gov't Trial Ex. 58; Trial Tr. 47, Dec. 13, 2013, ECF No. 332.

[2] Although the government's application and resulting court order sought 152 days of records (December 1, 2010 through May 2, 2011), MetroPCS produced 127 days of records (December 1, 2010 through April 6, 2011).

[3] Cell sites, which are the transmitting towers through which cell phones communicate with the telephone network, consist of antennas facing different directions that cover distinct wedge-shaped "sectors."

has a "roaming agreement . . . with Sprint, which does cover that area." Trial Tr. 59, Dec. 13, 2013. ECF No. 332.[4] Therefore, Sprint, not MetroPCS, possessed Carpenter's cell site location information for calls made and received while he was in Ohio. Sprint produced two pages of call detail records with cell site location information for March 3 and 4, 2011.

MetroPCS and Sprint also produced lists of their cell sites in southern Michigan and northwestern Ohio, respectively, providing the longitude, latitude, and physical address of each cell site, along with the directional orientation of each sector antenna. *See id.* at 74. By cross-referencing the information in Carpenter's call detail records with these cell-site lists, the government could identify the area in which Carpenter's phone was located and could thereby deduce Carpenter's location and movements at multiple points each day.

2. The precision of a cell phone user's location reflected in cell site location information ("CSLI") records depends on the size of the cell site sectors in the area. Most cell sites consist of multiple directional antennas that divide the cell site into "sectors." Pet. App. 5a. The coverage area of cell site sectors is smaller in areas with greater density of cell towers, with urban areas having the greatest density and thus the smallest coverage areas. *Id.*; *see also* Pet. App. 88a (Gov't Trial Ex. 57, at 13) (providing maps of MetroPCS and Sprint cell sites).

---

[4] As explained at trial, "[i]n a roaming situation, if [a service provider] doesn't have coverage in a particular area of the country, they would have an agreement with another company to be able to utilize their infrastructure." *Id.* at 39–40.

The density of cell sites continues to increase as data usage from smartphones grows. Because each cell site can carry only a fixed volume of data required for text messages, emails, web browsing, streaming video, and other uses, as smartphone data usage increases carriers must erect additional cell sites, each covering smaller geographic areas. *See* CTIA - The Wireless Association, *Annual Wireless Industry Survey* (2016)[5] (showing that the number of cell sites in the United States increased from 183,689 to 307,626 from 2005 to 2015); *id.* (annual wireless data usage increased from 388 billion megabytes to 9.65 trillion megabytes between 2010 and 2015). This means that in urban and dense suburban areas like Detroit, many sectors cover small geographic areas and therefore can provide relatively precise information about the location of a phone. Pet. App. 5a.

Although in this case MetroPCS provided only information identifying Carpenter's cell site and sector at the start and end of his calls, service providers increasingly retain more granular historical location data, including for text messages and data connections. *United States v. Davis*, 785 F.3d 498, 542 (11th Cir. 2015) (en banc) (Martin, J., dissenting). Location precision is also increasing as service providers deploy millions of "small cells," "which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home." *United States v. Graham*, 824 F.3d 421, 448 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in

---

[5] *Available at* http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

part and concurring in the judgment) (citation omitted).

3. Before trial, Carpenter joined his codefendant's motion to suppress the CSLI records on the basis that their acquisition pursuant to the "'reasonable grounds standard' in the Stored Communications Act . . . is unconstitutional." Pet. App. 36a; *see also id.* at 4a. Relying on *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), a case holding that no warrant is required for short-term real-time tracking of a suspect's cell phone, the district court denied the motion on the basis that acquisition of the cell-site records was not a Fourth Amendment search. Pet. App. 38a–39a.

At trial, the government introduced information about Carpenter's CSLI records and relied on them to establish Carpenter's location on the days of the charged robberies. FBI Special Agent Christopher Hess testified that Carpenter's CSLI records placed him near the sites of four of the robberies. Pet. App. 5a–6a. Hess also produced maps showing the location of Carpenter's phone relative to the locations of the robberies, which the government introduced into evidence. Pet. App. 6a; *Id.* at 86a–89a (Gov't Trial Ex. 57). The government relied on the records to show Carpenter's proximity to "the robberies around the time the robberies happened." Pet. App. 6a. The prosecutor argued to the jury, for example, that Mr. Carpenter was "right where the first robbery was at the exact time of the robbery, the exact sector," Trial Tr. 56, Dec. 16, 2013, ECF No. 333, and that he was "right in the right sector before the Radio Shack in Highland Park," *id. See also* Trial

Tr. 49 62, Dec. 13, 2013, ECF No. 332 (testimony of Special Agent Hess).

The jury convicted Carpenter of six robberies in violation of the Hobbs Act, 18 U.S.C. § 1951(a), and five separate violations of 18 U.S.C. § 924(c) for using or carrying a firearm in connection with a federal crime of violence and aiding and abetting. All but the first of the § 924(c) convictions carried mandatory consecutive minimum sentences of 25 years each. As a result, the court sentenced Carpenter to nearly 116 years' imprisonment (1,395 months).

5. On appeal, a divided three-judge panel of the Sixth Circuit held that no search occurred under the Fourth Amendment because Carpenter had no reasonable expectation of privacy in cell phone location records held by his service provider. Pet. App. 17a. Writing for the majority, Judge Kethledge concluded that people do not have a reasonable expectation of privacy in CSLI because it is a business record of the service provider that reveals routing information rather than the contents of communications. Pet. App. 10a–11a. Judge Kethledge relied in part on this Court's 1979 decision in *Smith v. Maryland*, 442 U.S. 735 (1979), reasoning that like the dialed phone numbers conveyed to the phone company in *Smith*, people knowingly expose their location information to their service provider and therefore lack an expectation of privacy in it. Pet. App. 11a–12a.

Judge Stranch disagreed. Concurring in the judgment only, she explained that "the sheer quantity of sensitive information procured without a warrant in this case raises Fourth Amendment

concerns of the type the Supreme Court . . . acknowledged in *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring)." Pet. App. 24a. "I do not think that treating the CSLI obtained as a 'business record' and applying that test addresses our circuit's stated concern regarding long-term, comprehensive tracking of an individual's location without a warrant." *Id.* at 29a. Judge Stranch concluded, however, that suppression was not warranted under the good-faith exception to the exclusionary rule, a question that the majority did not address. *Id.* at 29a-31a. On that alternative basis, she concurred in the judgment.

REASONS FOR GRANTING THE WRIT

I. THIS CASE PRESENTS AN IMPORTANT AND RECURRING QUESTION ON THE SCOPE OF CONSTITUTIONAL PRIVACY RIGHTS IN THE DIGITAL AGE.

A. The Lower Courts Have Expressly and Repeatedly Sought This Court's Guidance in Addressing the Question Presented.

The question at the center of this case—whether there is a reasonable expectation of privacy under the Fourth Amendment in a person's cell site location information held by their cellular service provider—requires definitive resolution by this Court. Numerous lower court judges addressing the issue have explained that they feel bound by this Court's third-party-doctrine cases from the 1970s, but that they are discomfited by the result they believe those cases require them to reach. Only this Court can provide the guidance they seek about

whether and how a doctrine developed long before the digital age applies to the voluminous and sensitive digital records at issue here. More specifically, only this Court can determine whether *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), render the Fourth Amendment irrelevant when the government seeks detailed records from a cell phone provider cataloging the location and movements of a cell phone user over many months.

In *Smith*, this Court ruled that the short-term use of a pen register to capture the telephone numbers a person dials is not a search under the Fourth Amendment. 442 U.S. at 742. The Court relied heavily on the fact that when dialing a phone number, the caller "voluntarily convey[s] numerical information to the telephone company." *Id.* at 744. The Court also assessed the degree of invasiveness of the surveillance to determine whether the user had a reasonable expectation of privacy. The Court noted the "pen register's limited capabilities," *id.* at 742, explaining that "a law enforcement official could not even determine from the use of a pen register whether a communication existed." *Id.* at 741 (citation omitted). Similarly, in *Miller*, the Court concluded that bank customers do not have any Fourth Amendment interest in their bank records because all the information in those records has been voluntarily conveyed to the bank. 425 U.S. 435, 440 42 (1976). The principle sometimes discerned from these cases, that certain records or information shared with third parties deserve no Fourth Amendment protection, is known as the "third-party doctrine."

Lacking further guidance from this Court, lower courts have been struggling to apply the pre-digital holdings in *Smith* and *Miller* to newer forms of pervasive digital data.

In *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc), *cert. denied*, 136 S. Ct. 479 (2015), for example, a majority of the en banc Eleventh Circuit held that this Court's decisions in *Smith* and *Miller* require the conclusion that there is no Fourth Amendment protection for CSLI records. But while the Eleventh Circuit believed it "remains bound by *Smith* and *Miller*," 785 F.3d at 514, two separate concurrences called on this Court to clarify the scope of those decisions, evincing discomfort with their application to the records at issue. As Judge Rosenbaum wrote:

> In our time, unless a person is willing to live "off the grid," it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling. . . . Since we are not the Supreme Court and the third-party doctrine continues to exist and to be good law at this time, though, we must apply the third-party doctrine where appropriate.

Id. at 525 (Rosenbaum, J., concurring); *see also id.* at 519, 521 (William Pryor, J., concurring) ("[W]e must leave to the Supreme Court the task of developing

exceptions to the rules it has required us to apply. . . . As judges of an inferior court, we have no business in anticipating future decisions of the Supreme Court. If the third-party doctrine results in an unacceptable 'slippery slope,' the Supreme Court can tell us as much. That is, if 'the Supreme Court has given reasons to doubt the rule's breadth,' it alone must decide the exceptions to its rule." (citations omitted)).

Likewise, the en banc majority of the Fourth Circuit wrote that "[t]he Supreme Court may in the future limit, or even eliminate, the third-party doctrine. . . . But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case." *United States v. Graham*, 824 F.3d 421, 425 (4th Cir. 2016) (en banc). And in this case, Judge Stranch discussed her "concern[] about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled," concluding that there is a "need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances." Pet. App. 29a (Stranch, J., concurring).

All told, the five courts of appeals to consider the Fourth Amendment status of historical CSLI have generated 18 separate majority, concurring, and dissenting opinions, highlighting the need for this Court to act. *See* Pet. App. 1a (majority opinion); *id.* at 24a (Stranch, J., concurring); *United States v. Graham*, 824 F.3d 421, 424 (4th Cir. 2016) (en banc) (majority opinion); *id.* at 438 (Wilkinson, J., concurring); *id.* at 441 (Wynn, J., dissenting in part

and concurring in the judgment); *United States v. Graham*, 796 F.3d 332, 338 (4th Cir. 2015) (majority opinion), *vacated, reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015); *id.* at 377 (Thacker, J., concurring); *id.* at 378 (Motz, J., dissenting in part and concurring in the judgment); *United States v. Davis*, 785 F.3d 498, 500 (11th Cir. 2015) (en banc) (majority opinion); *id.* at 519 (William Pryor, J., concurring); *id.* at 521 (Jordan, J., concurring); *id.* at 524 (Rosenbaum, J., concurring); *id.* at 533 (Martin, J., dissenting); *United States v. Davis*, 754 F.3d 1205, 1208 (11th Cir. 2014) (unanimous), *vacated, reh'g en banc granted*, 573 F. App'x 925 (11th Cir. 2014); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 602 (5th Cir. 2013) [*"Fifth Circuit CSLI Opinion"*] (majority opinion); *id.* at 615 (Dennis, J., dissenting); *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 305 (3d Cir. 2010) [*"Third Circuit CSLI Opinion"*] (majority opinion); *id.* at 319 (Tashima, J., concurring).

As reflected in these 18 opinions attempting to grapple with the same basic issue, lower courts are divided over how to apply the third-party doctrine to CSLI records. *Compare Graham*, 824 F.3d at 424–25 (no expectation of privacy in CSLI under *Smith*), *Davis*, 785 F.3d at 511–13 (same), *and Fifth Circuit CSLI Opinion*, 724 F.3d at 612–13 (same), *with Third Circuit CSLI Opinion*, 620 F.3d at 317 (distinguishing *Smith* and holding that cell phone users may retain a reasonable expectation of privacy in CSLI); *Zanders v. State*, No. 15A01–1509–CR–1519, __ N.E.3d __, 2016 WL 4140998, at *8–10 (Ind. Ct. App. Aug. 4, 2016) (distinguishing *Smith* and *Miller* and holding that "the third-party doctrine

does not dictate the outcome of this case"), *pet. to transfer jurisdiction to Indiana Supreme Court filed* (Sept. 6, 2016).

This struggle to define the scope of Fourth Amendment protection for newer forms of sensitive digital data reflects, at least in part, scholarly criticism of the expansive application of the third-party doctrine beyond the kinds of records at issue in *Smith* and *Miller*. *See, e.g.*, Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 Stan. L. Rev. 119 (2002); Daniel J. Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087, 1151–52 (2002). These scholars have joined the lower courts in calling on this Court to ensure that the Fourth Amendment keeps pace with the rapid advance of technology.

In sum, there is a substantial question of how the protections of the Fourth Amendment should apply to sensitive and private data in the hands of trusted third parties. As Justice Sotomayor noted in *United States v. Jones*,

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.

132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

It is not necessary in this case to reassess the continued validity of the third-party doctrine in every possible context. But it is critically important to clarify the scope of analog-age precedents to digital surveillance techniques. Without guidance from this Court, a cell phone user "cannot know the scope of his constitutional protection, nor can a policeman know the scope of his authority." *New York v. Belton*, 453 U.S. 454, 459–60 (1981). As law enforcement seeks ever greater quantities of location data and other sensitive digital records, the need for this Court to speak grows daily more urgent.

B. This Court's Recent Decisions Have Properly Recognized a Need to Reexamine Traditional Understandings of Privacy in the Digital Age.

Twice in recent terms this Court has confronted crucial questions regarding the application of the Fourth Amendment in the digital age. *See Riley v. California*, 134 S. Ct. 2473 (2014) (warrant required for search of cell phone seized incident to lawful arrest); *United States v. Jones*, 132 S. Ct. 945 (2012) (tracking car with GPS device is a Fourth Amendment search). This case presents an important next step in the ongoing effort to reconcile enduring Fourth Amendment principles with the reality of a new digital world.

In *United States v. Jones*, this Court addressed the pervasive location monitoring made possible by GPS tracking technology surreptitiously and warrantlessly attached to a vehicle. All members of the Court agreed that attaching a GPS device to a vehicle and tracking its movements constitutes a

search under the Fourth Amendment. In so holding, the Court made clear that the government's use of novel digital surveillance technologies not in existence at the framing of the Fourth Amendment does not escape the Fourth Amendment's reach. 132 S. Ct. at 950–51 ("[W]e must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001))); *id.* at 963–64 (Alito, J., concurring in the judgment) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

In *Riley v. California*, the Court addressed Americans' privacy rights in the contents of their cell phones, unanimously holding that warrantless search of the contents of a cell phone incident to a lawful arrest violates the Fourth Amendment. In so doing, the Court rejected the government's inapt analogy to other physical objects that have historically been subject to warrantless search incident to an arrest. 134 S. Ct. at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.").

Monitoring an individual's location and movements over an extended period of time by collecting and analyzing cell phone records can and frequently will expose extraordinarily sensitive details of a person's life including, potentially, "a wealth of detail about . . . familial, political, professional, religious, and sexual associations."

Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring). Without disputing that premise, the court of appeals nonetheless held that this voluminous documentation of a person's movements in public *and* private spaces is unprotected by the Fourth Amendment by analogizing to the kinds of limited analog data at issue in *Smith* and *Miller*. Pet. App. 11a–14a. As this Court recently cautioned, however, unexamined reliance on "pre-digital analogue[s]" risks causing "a significant diminution of privacy." *Riley*, 134 S.Ct. at 2493. Accordingly, "any extension of . . . reasoning [from decisions concerning analog searches] to digital data has to rest on its own bottom." *Id.* at 2489. Only this Court can make that ultimate constitutional judgment.

C. The Volume and Frequency of Warrantless Law Enforcement Requests for CSLI Highlights the Importance of the Question Presented.

"[M]ore than 90% of American adults . . . own a cell phone." *Riley*, 134 S. Ct. at 2490. As of December 2015, there were more than 377 million wireless subscriber accounts in the United States.[6] Forty-four percent of U.S. households have *only* cell phones.[7] When "nearly three-quarters of smart phone

---

[6] CTIA The Wireless Association, *Annual Wireless Industry Survey* (2016), http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

[7] Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January–June 2014* 1 (Dec. 2014), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201412.pdf.

users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower," *Riley*, 134 S. Ct. at 2490, the privacy implications of warrantless law enforcement access to cell phone location data are difficult to overstate.

This is not an isolated or occasional concern. Law enforcement is requesting staggering volumes of CSLI from service providers. From July 2015 to June 2016, for example, AT&T received 75,302 requests for cell phone location information.[8] Verizon received approximately 18,935 requests for cell phone location data in just the first half of 2016.[9]

The government often obtains large volumes of CSLI pursuant to such requests. In this case the government requested five months' and obtained nearly four months' (127 days') worth of Carpenter's location data comprising thousands of location data points. A request for months of data is no aberration: according to T-Mobile, which now owns Carpenter's service provider, MetroPCS, the average law enforcement request "asks for approximately fifty-five days of records."[10] Other recent and pending cases involve comparable or even greater quantities

---

[8] AT&T, *Transparency Report*, at 4 (2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT TransparencyReport_July2016.pdf .

[9] Verizon, *Transparency Report 1H 2016*, at 5 (2016), https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report US-1H-2016.pdf.

[10] T-Mobile, *Transparency Report for 2013 & 2014*, at 5 (2015), http://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf.

of sensitive location information obtained without a warrant. In one case, the government obtained 221 days (more than seven months) of cell site location information, revealing 29,659 location points for one defendant. *See Graham*, 824 F.3d at 446–47 (Wynn, J., dissenting in part and concurring in the judgment).

In *Jones*, Justice Alito recognized that of the "many new devices that permit the monitoring of a person's movements," cell phones are "[p]erhaps most significant." 132 S. Ct. at 963 (Alito, J., concurring in the judgment). Yet most law enforcement agencies are obtaining these large quantities of historical CSLI without a probable cause warrant. *See* American Civil Liberties Union, Cell Phone Location Tracking Public Records Request (Mar. 25, 2013)[11] (responses to public records requests sent to roughly 250 local law enforcement agencies show that "few agencies consistently obtain warrants" for CSLI). The volume of warrantless requests for CSLI and the ubiquity of cell phones make the question presented one of compelling national importance.

Judge Kozinski has summarized the situation well. In an opinion written six years ago, he began by noting that this Court's decision in *United States v. Knotts*, 460 U.S. 276, 283-84 (1983), expressly left open the question whether "'twenty-four hour surveillance of any citizen of this country' by means of 'dragnet-type law enforcement practices' violates the Fourth Amendment's guarantee of personal privacy." *United States v. Pineda-Moreno*, 617 F.3d

---

[11] https://www.aclu.org/cases/cell-phone-location-tracking-public-records-request.

1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing *en banc*). He then cogently observed, "[w]hen requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use." *Id.* What was true six years ago is even more true today. This Court's intervention is needed now to ensure that the Fourth Amendment does not become a dead letter as police accelerate their warrantless access to rich troves of sensitive personal location data.

II. FEDERAL COURTS OF APPEALS AND STATE HIGH COURTS ARE DIVIDED.

The Sixth Circuit's decision in this case widens the conflict over whether, or in what circumstances, sensitive cell phone location data held in trust by a service provider is protected by a warrant requirement.

A. The Circuits Are Split Over Whether the Third-Party Doctrine Eliminates People's Reasonable Expectation of Privacy in Their Historical CSLI.

The Sixth Circuit joins the Fourth, Fifth, and Eleventh Circuits in holding that there is no reasonable expectation of privacy in historical cell site location information under the Fourth Amendment, and therefore that no warrant is required. In the first of these decisions, *In re Application of the U.S. for Historical Cell Site Data*,

724 F.3d 600 (5th Cir. 2013), a magistrate judge rejected a government application for an order pursuant to the Stored Communications Act, 18 U.S.C. § 2703(d), seeking historical CSLI, holding that a warrant is required under the Fourth Amendment. On appeal, a divided panel of the Fifth Circuit held that any expectation of privacy in CSLI is vitiated by the cell service provider's creation and possession of the records. 724 F.3d at 613. The court rejected the argument that cell phone users retain an expectation of privacy in the data because they do not voluntarily convey their location information to the service provider. *Id.* at 613–14; *see also United States v. Guerrero*, 768 F.3d 351, 358–59 (5th Cir. 2014) (applying *In re Application* in the context of a suppression motion). The Fourth and Eleventh Circuits have subsequently agreed with this position. *Graham*, 824 F.3d at 424–25; *Davis*, 785 F.3d at 511–13.

The Third Circuit takes the contrary position. *See Fifth Circuit CSLI Opinion*, 724 F.3d at 616 (Dennis, J., dissenting) (recognizing split between Third and Fifth Circuits). In a decision issued more than a year before this Court's opinion in *Jones*, the Third Circuit held that magistrate judges have discretion to require a warrant for historical CSLI if they determine that the location information sought will implicate the suspect's Fourth Amendment privacy rights by showing, for example, when a person is inside a constitutionally protected space. *Third Circuit CSLI Opinion*, 620 F.3d at 319. In reaching that conclusion, the court rejected the argument that a cell phone user's expectation of privacy is eliminated by the service provider's ability to access that information:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."

Id. at 317–18 (last alteration in original). Therefore, the court held, the third-party doctrine does not apply to historical CSLI records. *Id.*

This split in the circuits is accentuated by the growing number of states that require a warrant for historical CSLI by statute or pursuant to judicial opinion. *See Zanders v. State*, No. 15A01–1509–CR–1519, __ N.E.3d __, 2016 WL 4140998 (Ind. Ct. App. Aug. 4, 2016); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); Colo. Rev. Stat. § 16-3-303.5(2); Me. Rev. Stat. tit. 16, § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); Utah Code Ann. § 77-23c-102(1)(a); N.H. Rev. Stat. Ann. § 644-A:2; 2016 Vt. Laws No. 169 (S. 155) (to be codified at Vt. Stat. Ann. tit. 13, § 8102(b)). Additional states require a warrant for real-time cell phone location data. *See, e.g., Tracey v.*

State, 152 So. 3d 504 (Fla. 2014); *State v. Earls*, 70 A.3d 630 (N.J. 2013); 725 Ill. Comp. Stat. 168/10; Ind. Code 35-33-5-12; Md. Code Ann. Crim. Proc. § 1-203.1(b); Va. Code Ann. § 19.2-70.3(C). Requiring a warrant for CSLI would harmonize the protections available to people throughout the United States.

B. The Circuits Are Split Over Whether There is a Reasonable Expectation of Privacy in Longer-Term Location Information Collected by Electronic Means.

In *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945, the D.C. Circuit held that using a GPS device to surreptitiously track a car over the course of 28 days violates reasonable expectations of privacy and is therefore a Fourth Amendment search. *Id.* at 563. The court explained that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation." *Id.* at 562. Therefore, people have a reasonable expectation of privacy in the intimate and private information revealed by "prolonged GPS monitoring." *Id.* at 563.

Although this Court affirmed on other grounds, relying on a trespass-based rationale, the D.C. Circuit's approach under the *Katz* reasonable-expectation-of-privacy test remains controlling law in

that circuit.[12] And that holding does not depend on the nature of the tracking technology at issue: prolonged electronic surveillance of the location of a person's cell phone is at least as invasive as prolonged electronic surveillance of the location of her car. *See Jones*, 132 S. Ct. at 963 (Alito, J., concurring in the judgment) (explaining that law enforcement access to cell phone location information is "[p]erhaps most significant" of the "many new devices that permit the monitoring of a person's movements.").

The Sixth Circuit rejected this reasoning when it held that the information contained in CSLI records is categorically unprotected by the Fourth Amendment, regardless of what it reveals and over what period of time. Pet. App. 13a–14a. In doing so, the court of appeals widened the circuit split over whether people have a reasonable expectation of privacy in their longer-term location information—a split that existed prior to *Jones* and continues today. *Compare Maynard*, 615 F.3d at 563 (prolonged electronic location tracking is a search under the Fourth Amendment), *with Pineda-Moreno*, 591 F.3d at 1216–1217 (prolonged electronic location tracking is not a search under the Fourth Amendment), *United States v. Garcia*, 474 F.3d 994, 996–99 (7th Cir. 2007) (same), *and United States v. Marquez*, 605 F.3d 604, 609 (8th Cir. 2010) ("A person traveling via automobile on public streets has no reasonable

---

[12] *See* Will Baude, *Further Thoughts on the Precedential Status of Decisions Affirmed on Alternate Grounds*, The Volokh Conspiracy (Dec. 3, 2013, 7:27 PM), http://volokh.com/2013/12/03/thoughts-precedential-status-decisions-affirmed-alternate-grounds/.

expectation of privacy in his movements from one locale to another.").

III. THE SIXTH CIRCUIT ERRED IN HOLDING THAT THE CONDUCT HERE WAS NOT A SEARCH.

A. The Sixth Circuit Erred in Holding That There Is No Reasonable Expectation of Privacy in Historical CSLI.

The Sixth Circuit majority held that the mere fact that the government obtained the CSLI records from Petitioner's service provider, rather than from Petitioner himself, dooms his Fourth Amendment claim in light of *United States v. Miller* and *Smith v. Maryland*. Neither *Miller* nor *Smith* compels that conclusion and this Court should reject that understanding of its prior precedent. The mere fact that another person or entity has access to or control over private records does not in itself—and without regard to any other circumstance—destroy an otherwise reasonable expectation of privacy. Though third-party access to records may be one factor weighing on the *Katz* reasonable-expectation-of-privacy analysis, the third-party doctrine elucidated in *Miller* and *Smith* is not and never has been an on-off switch. *See Florida v. Jardines*, 133 S. Ct. 1409, 1418–19 (2013) (Kagan, J., concurring) (expectation of privacy in odors detectable by a police dog that emanate from a home); *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (information about location and movement in public, even though exposed to public view); *Kyllo*, 533 U.S. 27 (thermal signatures emanating from a home); *Ferguson v. City*

of Charleston, 532 U.S. 67, 78 (2001) ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."); *Bond v. United States*, 529 U.S. 334, 336 (2000) (bag exposed to the public on luggage rack of bus); *Minnesota v. Olson*, 495 U.S. 91, 98–99 (1990) ("an overnight guest has a legitimate expectation of privacy in his host's home" even though his possessions may be disturbed by "his host and those his host allows inside"); *United States v. Jacobsen*, 466 U.S. 109, 115 (1984) (reasonable expectation of privacy in letters and sealed packages entrusted to private freight carrier); *Katz v. United States*, 389 U.S. 347 (1967) (reasonable expectation of privacy in contents of phone call even though call is conducted over private companies' networks); *Stoner v. California*, 376 U.S. 483, 487–90 (1964) (implicit consent to janitorial personnel to enter motel room does not amount to consent for police to search room); *Chapman v. United States*, 365 U.S. 610, 616 17 (1961) (search of a house invaded tenant's Fourth Amendment rights even though landlord had authority to enter house for some purposes).

The Sixth Circuit erred in treating the fact of third party access to the records as dispositive. Pet. App. 14a. This Court should make clear that the reasonable-expectation-of-privacy test relies on a totality-of-the-circumstances analysis. Avoiding mechanical applications of holdings from the analog age is of paramount importance when dealing with highly sensitive and voluminous digitized records. *See Riley*, 134 S. Ct. at 2489. It is virtually impossible to participate fully in modern life without

leaving a trail of digital breadcrumbs that create a pervasive record of the most sensitive aspects of our lives. Ensuring that technological advances do not "erode the privacy guaranteed by the Fourth Amendment," *Kyllo*, 533 U.S. at 34, requires nuanced applications of analog-age precedents.

This is not to say that proper resolution of this case requires wholesale rejection of *Smith* and *Miller*'s holdings. Even on the plain terms of those decisions, Petitioner retains a reasonable expectation of privacy in his CSLI.

To assess an individual's expectation of privacy in records held by a third party this Court has looked to, among other factors, whether the records were "voluntarily conveyed" to that entity, *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 744, and what privacy interest a person has in the information the records reveal, *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 741–42. Unlike the dialed phone numbers and limited bank records at issue in *Smith* and *Miller*, "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." *Third Circuit CSLI Opinion*, 620 F.3d at 317. Location information is not entered by the user into the phone, nor otherwise affirmatively transmitted to the service provider. This is doubly true when a person receives a call, thereby taking *no* action that would knowingly or voluntarily reveal location. *Id.* at 317–18. It is also particularly clearly the case when that person's cell phone is roaming on another carrier's network, as was Carpenter's here, because "[t]ypically, a cell phone user does not know when her phone is roaming onto another provider's

network, much less the name of the other provider on whose network her phone is roaming." *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1028–29 (N.D. Cal. 2015), *appeal dismissed*, No. 15-16760 (9th Cir. Feb. 5, 2016). "As a result, cell phone users, unlike a bank depositor or telephone dialer, will often not know the identity of the third party to which they are supposedly conveying information." *Id.* at 1029.

Moreover, the documentation of a person's movements, locations, and activities over the course of time contained in CSLI records is exceedingly sensitive and private in ways that were not at issue in *Smith* or *Miller*. This is so for at least two reasons. First, because people carry their phones with them virtually everywhere they go, including inside their homes and other constitutionally protected spaces, cell phone location records can reveal information about presence, location, and activity in those spaces. *See United States v. Davis*, 754 F.3d 1205, 1215-16 (11th Cir. 2014) (Sentelle, J.), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015). In *United States v. Karo*, 468 U.S. 705 (1984), this Court held that location tracking implicates Fourth Amendment privacy interests when it may reveal information about individuals in areas where they have reasonable expectations of privacy. The Court explained that using an electronic device—there, a beeper—to infer facts about "location[s] not open to visual surveillance," like whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises, was just as unreasonable as physically searching the location without a warrant. *Id.* at 714–16. Such location tracking "falls

within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place. *Id.* at 707; *see also Kyllo*, 533 U.S. at 36 (use of thermal imaging device to learn information about interior of home constitutes a search).

Second, CSLI reveals a great sum of sensitive and private information about a person's movements and activities in public and private spaces that, at least over the longer term, violates expectations of privacy. In *Jones*, although the majority opinion relied on a trespass-based rationale to determine that a search had taken place, 132 S. Ct. at 949, it specified that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* [reasonable-expectation-of-privacy] analysis." *Id.* at 953. Five Justices conducted a *Katz* analysis, and concluded that at least longer-term location tracking violates reasonable expectations of privacy. *Id.* at 960, 964 (Alito, J., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring).

This conclusion did not depend on the particular type of tracking technology at issue in *Jones*. As Justice Sotomayor explained, electronic location tracking implicates the Fourth Amendment because it "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* at 955. This Court subsequently amplified that point when it explained that cell phone location data raises particularly acute privacy concerns because it "can reconstruct someone's specific movements down to

the minute, not only around town but also within a particular building." *Riley*, 134 S. Ct. at 2490 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

The records obtained by the government in this case implicate both the expectation of privacy in private spaces and the expectation of privacy in longer-term location information. They allow the government to know or infer when a person slept at home and when he didn't. *Davis*, 785 F.3d at 540–41 (Martin, J., dissenting). They show a person's movements around town, nearly down to the minute.[13] *Id.* They even allow the government to learn who a person associated with and when. *See, e.g.*, Pet. App. 81a–82a (concluding that co-defendants were at the same location based on their CSLI records); Trial Tr. 107, Dec. 16, 2013, ECF No. 333 (same).

It is not surprising, therefore, that polling data shows that more than 80 percent of people consider

---

[13] Even knowing only periodic information about which cell sites a phone connects to over time can be used to interpolate the path the phone user traveled, thus revealing information beyond just where the phone was located at discrete points. *See, e.g.*, Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Syss. Design & Implementation 20 (2011), https://www.usenix.org/legacy/events/nsdi11/tech/full_papers/Thiagarajan.pdf?CFID=23055068 5&CFTOKEN=76524860 (describing one algorithm for accurate trajectory interpolation using cell site information). Law enforcement routinely uses cell site data for this purpose; in this case, the government presented testimony explaining that cell site data points revealed Carpenter's trajectories placing him at the businesses in question at the relevant times. *See* Trial Tr. 55, 57, 62, Dec. 13, 2013, ECF No. 332.

"[d]etails of [their] physical location over time" to be "sensitive"—evincing greater concern over this information than over the contents of their text messages, a list of websites they have visited, or their relationship history.[14] Historical CSLI enables the government to "monitor and track our cell phones, and thus ourselves, with minimal expenditure of funds and manpower, [which] is just the type of gradual and silent encroachment into the very details of our lives that we as a society must be vigilant to prevent." *Tracey*, 152 So. 3d at 522 (internal quotation marks omitted).

B. The Sixth Circuit Erred In Deferring to Congress's 30-Year-Old Legislative Scheme.

In concluding that the Fourth Amendment does not protect people's cell site location records from warrantless search, the Sixth Circuit majority explained that "Congress has specifically legislated on the question before us today, and in doing so has struck the balance reflected in the Stored Communications Act." Pet. App. 15a. Thus, "society itself—in the form of its elected representatives in Congress—has already struck a balance that it thinks reasonable." *Id.* at 16a. Therefore, the majority wrote, "[t]here is considerable irony in [a] request" to "declare that balance unconstitutional." *Id.* at 15a.

---

[14] Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 32, 34 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

The supposed balance to which the majority refers is decades old, and is a relic of legislation passed before the proliferation of cell phones and the availability of large volumes of increasingly precise cell site location information. When Congress passed the Stored Communications Act in 1986,[15] there were a mere 1,000 cell sites in the United States[16] (compared to more than 300,000 today)[17] and less than one half of one percent of Americans had a cell phone.[18] Congress gave no indication that it even considered the existence of historical CSLI, not to mention the possibility that law enforcement might want to access it. When Congress amended the Stored Communications Act in 1994,[19] cellular networks were still fragmented and rudimentary, with less than 18,000 cell sites across the country.[20] Congress simply did not contemplate the contemporary ubiquity of cell phones and the volume

---

[15] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848.

[16] Andrea Meyer, *30th Anniversary of the First Commercial Cell Phone Call*, Verizon (Oct. 11, 2013), https://www.verizonwireless.com/news/article/2013/10/30th-anniversary-cell-phone.html and https://www.slideshare.net/slideshow/embed_code/27105077?rel=0

[17] CTIA – The Wireless Association, *Annual Wireless Industry Survey*.

[18] Meyer, *30th Anniversary of the First Commercial Cell Phone Call*.

[19] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 207, 108 Stat. 4279 (1994).

[20] *Background on CTIA's Wireless Industry Survey* 2, CTIA-The Wireless Association (2014), http://www.ctia.org/docs/default-source/Facts-Stats/ctia_survey_ye_2013_graphics-final.pdf.

and precision of CSLI when crafting the SCA. Courts should not give undue weight to this outdated legislative scheme in evaluating people's reasonable expectation of privacy under the Fourth Amendment.

Moreover, in concluding that acquisition of historical CSLI is a Fourth Amendment search, a court need not hold the Stored Communications Act unconstitutional. The SCA contains a mechanism for law enforcement to obtain a warrant for CSLI. *See* 18 U.S.C. § 2703(c)(1)(A). "Section 2703(c) may be fairly construed to provide for 'warrant procedures' to be followed when the government seeks customer records that may be protected under the Fourth Amendment, including historical cell site location information." *Fifth Circuit CSLI Opinion*, 724 F.3d at 617 (Dennis, J., dissenting). The determination that "one proposed interpretation or use of the SCA as applied did not comply with the Fourth Amendment's requirement for a warrant based on probable cause" is firmly within the purview of the judiciary. Pet. App. 32a (Stranch, J., concurring). Indeed, "[t]he question before [the court] is one that courts routinely answer: did the search at issue require a warrant?" *Id.* at 31a–32a. This Court should provide a "simple" answer—"get a warrant." *Riley*, 134 S. Ct. at 2495.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully Submitted,

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Steven R. Shapiro
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street,
Suite 1400
Detroit, MI 48226

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES
UNION FUND OF
MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Dated: September 26, 2016

APPENDIX

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

United States of America,

Plaintiff-Appellee,

v.

No. Nos. 14-1572/1805

Timothy Ivory Carpenter (14-1572);
Timothy Michael Sanders (14-1805),

Defendants-Appellants.

Appeal from the United States District Court
For the Eastern District of Michigan at Detroit.
No. 2:12-cr-20218— Sean F. Cox, District Judge.

Argued: October 14, 2015

Decided and Filed: April 13, 2016

Before: GUY, KETHLEDGE, and STRANCH, Circuit Judges.

COUNSEL

ARGUED: Nathan Freed Wessler, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York, for Amicus Curiae. Harold Gurewitz, GUREWITZ & RABEN, PLC, Detroit, Michigan, for Appellant in 14-1572. Evan Howard Caminker, UNITED STATES ATTORNEY'S OFFICE, Detroit, Michigan, for Appellee. **ON BRIEF:** Harold Gurewitz, GUREWITZ & RABEN, PLC, Detroit, Michigan, for Appellant in

14-1572. S. Allen Early, LAW OFFICE OF S. ALLEN EARLY, Detroit, Michigan, for Appellant in 14-1805. Evan Howard Caminker, UNITED STATES ATTORNEY'S OFFICE, Detroit, Michigan, for Appellee. Nathan Freed Wessler, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York, Daniel S. Korobkin, Michael J. Steinberg, AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN, Detroit, Michigan, Rachel Levinson-Waldman, Michael W. Price, BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW, New York, New York, for Amicus Curiae.

KETHLEDGE, J., delivered the opinion of the court in which GUY, J., joined. STRANCH, J., joined the opinion in part and the result in part. STRANCH, J. (pp. 17–22), delivered a separate opinion joining in Parts II.B and III of the majority opinion and concurring in the judgment only with respect to Part II.A.

OPINION

KETHLEDGE, Circuit Judge. In Fourth Amendment cases the Supreme Court has long recognized a distinction between the content of a communication and the information necessary to convey it. Content, per this distinction, is protected under the Fourth Amendment, but routing information is not. Here, Timothy Carpenter and Timothy Sanders were convicted of nine armed robberies in violation of the Hobbs Act. The

government's evidence at trial included business records from the defendants' wireless carriers, showing that each man used his cellphone within a half-mile to two miles of several robberies during the times the robberies occurred. The defendants argue that the government's collection of those records constituted a warrantless search in violation of the Fourth Amendment. In making that argument, however, the defendants elide both the distinction described above and the difference between GPS tracking and the far less precise locational information that the government obtained here. We reject the defendants' Fourth Amendment argument along with numerous others, and affirm the district court's judgment.

I.

In April 2011, police arrested four men suspected of committing a string of armed robberies at Radio Shacks and T-Mobile stores in and around Detroit. One of the men confessed that the group had robbed nine different stores in Michigan and Ohio between December 2010 and March 2011, supported by a shifting ensemble of 15 other men who served as getaway drivers and lookouts. The robber who confessed to the crimes gave the FBI his own cellphone number and the numbers of other participants; the FBI then reviewed his call records to identify still more numbers that he had called around the time of the robberies.

In May and June 2011, the FBI applied for three orders from magistrate judges to obtain "transactional records" from various wireless carriers for 16 different phone numbers. As part of those applications, the FBI recited that these records

included "[a]ll subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target telephones from December 1, 2010 to present[,]" as well as "cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls[.]" The FBI also stated that these records would "provide evidence that Timothy Sanders, Timothy Carpenter and other known and unknown individuals" had violated the Hobbs Act, 18 U.S.C. § 1951. The magistrates granted the applications pursuant to the Stored Communications Act, under which the government may require the disclosure of certain telecommunications records when "specific and articulable facts show[] that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

The government later charged Carpenter with six counts, and Sanders with two, of aiding and abetting robbery that affected interstate commerce, in violation of the Hobbs Act, and aiding and abetting the use or carriage of a firearm during a federal crime of violence. *See* 18 U.S.C. §§ 924(c), 1951(a). Before trial, Carpenter and Sanders moved to suppress the government's cell-site evidence on Fourth Amendment grounds, arguing that the records could be seized only with a warrant supported by probable cause. The district court denied the motion.

At trial, seven accomplices testified that Carpenter organized most of the robberies and often supplied the guns. They also testified that Carpenter and his half-brother Sanders had served as lookouts during the robberies. According to these witnesses, Carpenter typically waited in a stolen car across the street from the targeted store. At his signal, the robbers entered the store, brandished their guns, herded customers and employees to the back, and ordered the employees to fill the robbers' bags with new smartphones. After each robbery, the team met nearby to dispose of the guns and getaway vehicle and to sell the stolen phones.

FBI agent Christopher Hess offered expert testimony regarding the cell-site data provided by Carpenter's and Sanders's wireless carriers, MetroPCS and T-Mobile. Hess explained that cellphones work by establishing a radio connection with nearby cell towers (or "cell sites"); that phones are constantly searching for the strongest signal from those towers; and that individual towers project different signals in each direction or "sector," so that a cellphone located on the north side of a cell tower will use a different signal than a cellphone located on the south side of the same tower. Hess said that cell towers are typically spaced widely in rural areas, where a tower's coverage might reach as far as 20 miles. In an urban area like Detroit, however, each cell site covers "typically anywhere from a half-mile to two miles." He testified that wireless carriers typically log and store certain call-detail records of their customers' calls, including the date, time, and length of each call; the phone numbers engaged on the call; and the cell sites

where the call began and ended.

With the cell-site data provided by Carpenter's and Sanders's wireless carriers, Hess created maps showing that Carpenter's and Sanders's phones were within a half-mile to two miles of the location of each of the robberies around the time the robberies happened. Hess used MetroPCS call-detail records, for example, to show that Carpenter was within that proximity of a Detroit Radio Shack that was robbed around 10:35 a.m. on December 13, 2010. Specifically, MetroPCS records showed that at 10:24 a.m. Carpenter's phone received a call that lasted about four minutes. At the start and end of the call, Carpenter's phone drew its signal from MetroPCS tower 173, sectors 1 and 2, located southwest of the store and whose signals point north-northeast. After the robbery, Carpenter placed an eight-minute call originating at tower 145, sector 3, located northeast of the store, its signal pointing southwest; when the call ended, Carpenter's phone was receiving its signal from tower 164, sector 1, alongside Interstate 94, north of the Radio Shack. *See* Carpenter App'x at 11. Hess provided similar analysis concerning the locations of Carpenter's and Sanders's phones at the time of a December 18, 2010 robbery in Detroit; a March 4, 2011 robbery in Warren, Ohio; and an April 5, 2011 robbery in Detroit. *See* Carpenter App'x at 12-15.

The jury convicted Carpenter and Sanders on all of the Hobbs Act counts and convicted Carpenter on all but one of the § 924(c) gun counts. Carpenter's convictions on the § 924(c) counts subjected him to four mandatory-minimum prison sentences of 25 years, each to be served

consecutively, leaving him with a Sentencing Guidelines range of 1,395 to 1,428 months' imprisonment. The district court sentenced Carpenter to 1,395 months' imprisonment and Sanders to 170 months' imprisonment. Carpenter and Sanders now appeal their convictions and sentences.

II.

A.

Carpenter and Sanders challenge the district court's denial of their motion to exclude their cell-site data from the evidence at trial. Those data themselves took the form of business records created and maintained by the defendants' wireless carriers: when the defendants made or received calls with their cellphones, the phones sent a signal to the nearest cell-tower for the duration of the call; the providers then made records, for billing and other business purposes, showing which towers each defendant's phone had signaled during each call. The government thereafter collected those records, and hence these cell-site data, for a range of dates (127 days of records for Carpenter, 88 days for Sanders) encompassing the robberies at issue here. The government did so pursuant to a court order issued under the Stored Communications Act, which required the government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). Carpenter and Sanders argue that the Fourth Amendment instead required the government to obtain a search warrant, pursuant to a showing of probable cause,

before collecting the data. The district court rejected that argument, holding that the government's collection of cell-site records created and maintained by defendants' wireless carriers was not a search under the Fourth Amendment. We review the district court's decision de novo. *See United States v. Lee*, 793 F.3d 680, 684 (6th Cir. 2015).

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]" U.S. Const. amend. IV. "[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *United States v. Jones*, 132 S.Ct 945, 950 (2012). Government trespasses upon those areas normally count as a search. *Id.* In *Katz v. United States*, 389 U.S. 347 (1967), however, the Supreme Court moved beyond a property-based understanding of the Fourth Amendment, to protect certain expectations of privacy as well. To fall within these protections, an expectation of privacy must satisfy "a twofold requirement": first, the person asserting it must "have exhibited an actual (subjective) expectation of privacy"; and second, that expectation must "be one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). When an expectation of privacy meets both of these requirements, government action that "invade[s]" the expectation normally counts as a search. *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

This case involves an asserted privacy interest in information related to personal communications. As to that kind of information, the federal courts have long recognized a core distinction: although the content of personal communications is private, the information necessary to get those communications from point A to point B is not. For example, in *Ex parte Jackson*, 96 U.S. 727, 733 (1878), the Court held that postal inspectors needed a search warrant to open letters and packages, but that the "outward form and weight" of those mailings— including, of course, the recipient's name and physical address—was not constitutionally protected. *Id.* That was true even though that information could sometimes bring embarrassment: "In a small village, for instance, a young gentleman may not altogether desire that all the loungers around the store which contains the Post-office shall be joking about the fair object of his affections." *Our Letters*, N.Y. Times, Dec. 12, 1872, at 4.

In the twentieth century, the telephone call joined the letter as a standard form of communication. The law eventually followed, recognizing that police cannot eavesdrop on a phone call—even a phone call placed from a public phone booth—without a warrant. *See Katz*, 389 U.S. at 352-55. But again the Supreme Court distinguished between a communication's content and the information necessary to send it. In *Katz*, the Court held that "[t]he Government's activities in electronically listening to and recording the petitioner's *words*" was a search under the Fourth Amendment. *Id.* at 353 (emphasis added). But in *Smith*, the Court held that the police's installation of

a pen register—a device that tracked the phone numbers a person dialed from his home phone—was not a search because the caller could not reasonably expect those numbers to remain private. "Although [the caller's] conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." *Smith*, 442 U.S. at 743 (emphasis in original).

Today, the same distinction applies to internet communications. The Fourth Amendment protects the content of the modern-day letter, the email. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). But courts have not (yet, at least) extended those protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like sender and recipient addresses on an email, or IP addresses. *See, e.g., United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007).

The business records here fall on the unprotected side of this line. Those records say nothing about the content of any calls. Instead the records include routing information, which the wireless providers gathered in the ordinary course of business. Carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls. And carriers keep records of these data to find weak spots in their network and to determine whether roaming charges apply, among other purposes. Thus,

the cell-site data –like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves. The government's collection of business records containing these data therefore is not a search.

The Supreme Court's decision in *Smith* confirms the point. At the outset, the Court observed that Smith could not claim that "his 'property' was invaded" by the State's actions, which meant he could not claim any property-based protection under the Fourth Amendment. And as to privacy, the Court hewed precisely to the content-focused distinction that we make here. 442 U.S. at 741. The Court emphasized (literally) that the State's pen register did "not acquire the *contents* of communications." *Id.* (emphasis in original). Instead, the Court observed, the phone numbers acquired by the State had been dialed "as a means of establishing communication." *Id.* Moreover, the Court pointedly refused to adopt anything like a "least- sophisticated phone user" (to paraphrase the Fair Debt Collection Practices Act) standard in determining whether phone users know that they convey that information to the phone company: "All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. The Court likewise charged "telephone users" with knowledge that "the phone company has facilities for recording" numerical information and that "the phone company does in fact record this information for a variety of legitimate business purposes." *Id.* at

743. Thus, the Court held, Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." 442 U.S. at 744. Hence the numerical information was not protected under the Fourth Amendment.

The same things are true as to the locational information here. The defendants of course lack any property interest in cell-site records created and maintained by their wireless carriers. More to the point, when the government obtained those records, it did "not acquire the *contents* of communications." *Id.* at 741. Instead, the defendants' cellphones signaled the nearest cell towers—thereby giving rise to the data obtained by the government here—solely "as a means of establishing communication." *Id.* Moreover, any cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone "exposes" its location to the nearest cell tower and thus to the company that operates the tower. *Accord United States v. Davis*, 785 F.3d 498, 511 (11th Cir. 2015) (en banc); *In re Application for Historical Cell Site Data*, 724, F.3d 600, 614 (5th Cir. 2013). And any cellphone user who has paid "roaming" (*i.e.*, out-of-network) charges—or even cellphone users who have not— should know that wireless carriers have "facilities for recording" locational information and that "the phone company does in fact record this information for a variety of legitimate business purposes." *Id.* at 743. Thus, for the same reasons that Smith had no expectation of privacy in the numerical information at issue there, the defendants have no such expectation in the locational information here. On this point, *Smith* is

binding precedent.

The defendants and their amicus, the American Civil Liberties Union, argue that *Jones* liberates us to hold otherwise. In *Jones*, five Justices (though not the Court in its majority opinion) agreed that "longer term GPS monitoring in government investigations of most offenses impinges on expectations of privacy." 132 S. Ct. at 964 (Alito, J., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring) (same). But there are at least two problems with the defendants' argument as made here. The first is that the government action in this case is very different from the government action in *Jones*. That distinction matters: in applying *Katz*, "it is important to begin by specifying *precisely the nature of the state activity that is challenged*." *Smith*, 442 U.S. at 741 (emphasis added). Whether a defendant had a legitimate expectation of privacy in certain information depends in part on what the government did to get it. A phone conversation is private when overheard by means of a wiretap; but that same conversation is unprotected if an agent is forced to overhear it while seated on a Delta flight. Similarly, information that is not particularly sensitive—say, the color of a suspect's vehicle—might be protected if government agents broke into the suspect's garage to get it. Yet information that is highly sensitive—say, all of a suspect's credit-charges over a three-month period—is not protected if the government gets that information through business records obtained per a subpoena. *See United States v. Phibbs*, 999 F.2d 1053, 1077-78 (6th Cir. 1993).

This case involves business records obtained from a third party, which can only diminish the defendants' expectation of privacy in the information those records contain. *See United States v. Miller*, 425 U.S. 435, 443 (1976); *Phibbs*, 999 F.2d at 1077-78. *Jones*, in contrast, lands near the other end of the spectrum: there, government agents secretly attached a GPS device to the underside of Jones's vehicle and then monitored his movements continuously for four weeks. That sort of government intrusion presents one set of Fourth Amendment questions; government collection of business records presents another. And the question presented here, as shown above, is answered by *Smith*.

The second problem with the defendants' reliance on *Jones* is that—unlike *Jones* this is not a GPS-tracking case. GPS devices are accurate within about 50 feet, which is accurate enough to show that the target is located within an individual building. Data with that kind of accuracy might tell a story of trips to "the strip club, the criminal defense attorney, the by-the- hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on[.]" *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (internal quotation marks omitted). But here the cell-site data cannot tell that story. Instead, per the undisputed testimony at trial, the data could do no better than locate the defendants' cellphones within a 120- (or sometimes 60-) degree radial wedge extending between one-half mile and two miles in length. Which is to say the locational data here are accurate within a 3.5 million square-foot to 100 million square-foot area—as much as 12,500 times less accurate than the

GPS data in *Jones*. And cell phone locational data are even less precise in suburban and rural settings. Areas of this scale might encompass bridal stores and Bass Pro Shops, gay bars and straight ones, a Methodist church and the local mosque. The ACLU responds that so-called "femtocells" can provide service (and thus identify a phone's location) within areas as small as ten meters. But our task is to decide this case, not hypothetical ones; and in this case there are no femtocells to be found. The defendants' argument is without merit.

The defendants similarly rely on *Riley v. California*, 134 S. Ct 2473, 2485 (2014), where the Court held the government may not access a smartphone's internal data - or, one might say, its contents -- without a warrant. But the Court's rationale was that smartphones typically store vast amounts of information about their users—vastly more, of course, than whether the user happens to be located within a two-mile radial wedge. *Riley* only illustrates the core distinction we make here.

Some other points bear mention. One is that Congress has specifically legislated on the question before us today, and in doing so has struck the balance reflected in the Stored Communications Act. The Act stakes out a middle ground between full Fourth Amendment protection and no protection at all, requiring that the government show "reasonable grounds" but not "probable cause" to obtain the cell-site data at issue here. *See* 18 U.S.C. § 2703(d). The defendants and the ACLU effectively ask us to declare that balance unconstitutional. There is considerable irony in that request. The *Katz* standard asks whether the defendants' asserted

expectation of privacy "is 'one that society is prepared to recognize as reasonable[.]'" *Smith*, 442 U.S. at 740 (quoting *Katz*, 389 U.S. at 361). Here, one might say that society itself—in the form of its elected representatives in Congress—has already struck a balance that it thinks reasonable. That is not to say that courts should defer to Congress's judgment on constitutional questions. But when the question itself turns on society's views, and society has in a meaningful way already expressed them, judges should bring a certain humility to the task of deciding whether those views are reasonable—lest judges "confuse their own expectations of privacy," *Jones*, 132 S. Ct. at 962 (Alito, J., concurring), with those that every reasonable person must hold.

A second point is related. Constitutional judgments typically rest in part on a set of empirical assumptions. When those assumptions concern subjects that judges know well—say, traffic stops—courts are well-equipped to make judgments that strike a reasonable balance among the competing interests at stake. *See* Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case For Caution, 102 Mich. L. Rev. 801, 863 (2004). But sometimes new technologies—say, the latest iterations of smartphones or social media—evolve at rates more common to superbugs than to large mammals. In those situations judges are less good at evaluating the empirical assumptions that underlie their constitutional judgments. Indeed the answers to those empirical questions might change as quickly as the technology itself does. With regard to the *Katz* test in particular, for example, "[d]ramatic

technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes." *Jones*, 132 S. Ct. at 962 (Alito, J., concurring). Congress is usually better equipped than courts are to answer the empirical questions that such technologies present. Thus, "[w]hen technologies are new and their impact remains uncertain, statutory rules governing law enforcement powers will tend to be more sophisticated, comprehensive, forward-thinking, and flexible than rules created by the judicial branch." Kerr, 102 Mich. L. Rev. at 859-60. These concerns favor leaving undisturbed the Congressional judgment here.

In sum, we hold that the government's collection of business records containing cell-site data was not a search under the Fourth Amendment.

B.

Sanders argues that the district court should have suppressed the government's cell-site evidence for another reason, namely that (in his view) the government's applications to obtain the cell-site records failed to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). There are several problems with that argument, but the simplest is that suppression of evidence is not among the remedies available under the Stored Communications Act. Quite the contrary: the statute identifies a handful of civil remedies, including "damages" and "equitable or declaratory relief," 18 U.S.C. § 2707(b), and

provides that those "are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708; *see United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014). The relief that Sanders seeks is therefore unavailable under the Act. *See United States v. Abdi*, 463 F.3d 547, 556 (6th Cir. 2006).

III.

A.

Carpenter argues that the district court erred when it denied Carpenter's motion for acquittal for lack of venue over counts seven and eight. Those counts charged Carpenter with aiding and abetting a Hobbs Act robbery in Warren, Ohio, and with aiding and abetting the use of a firearm in connection with that robbery. *See* 18 U.S.C. §§ 924(c), 1951(a). We review the district court's decision de novo. *See United States v. Kuehne*, 547 F.3d 667, 677 (6th Cir. 2008).

Carpenter was prosecuted in the Eastern District of Michigan. Venue was proper there so long as a rational trier of fact, viewing the evidence in the light most favorable to the government, could find by a preponderance of the evidence that any of Carpenter's accessorial acts, or the underlying crime itself, occurred in the Eastern District of Michigan. Relatedly, "[w]here venue is appropriate for the underlying crime of violence, so too it is for the § 924(c)(1) offense." *United States v. Rodriguez-Moreno*, 526 U.S. 275, 282 (1999).

Here, Carpenter's accomplices testified that, while in the Eastern District of Michigan,

Carpenter recruited the robbers for the Warren robbery, described for them the robbery's general scheme, and from there drove them to Ohio. Two of these witnesses also testified that, while in Michigan, Carpenter made arrangements to have another accomplice supply the robbers with a gun when they got to Warren. A reasonable trier of fact could credit this testimony, and conclude that much of Carpenter's conduct in abetting both the Warren robbery and the use of a firearm during it took place in the Eastern District of Michigan. The district court correctly denied Carpenter's motion for acquittal on counts seven and eight.

B.

Carpenter argues that the district court should have allowed him to use a report prepared by FBI Special Agent Vicente Ruiz to refresh the memory of government witness Adriane Foster on cross-examination. We review that evidentiary ruling for an abuse of discretion. *See United States v. Morales*, 687 F.3d 697, 701 (6th Cir. 2012).

At trial, Carpenter's counsel cross-examined Foster—an accomplice of Carpenter - about Foster's past statements to Agent Ruiz. Foster testified that he told Ruiz that Carpenter had provided Foster with advance information about the robbery in Warren. According to Ruiz's written summary of the interview, however, Foster told Ruiz that Sanders, not Carpenter, had provided Foster with advance information about the robbery. Carpenter's counsel sought to introduce Ruiz's report to "refresh [Foster's] memory" of the interview.

A document may be used to refresh a witness's memory only after his memory has been "exhausted." *Rush v. Ill. Cent. R.R. Co.*, 399 F.3d 705, 716 (6th Cir. 2005). Here, Foster seemed to have no trouble remembering his conversation with Agent Ruiz. Foster repeatedly testified that he did remember telling Ruiz that Timothy Carpenter—not Timothy Sanders—had told him about the plans for the Warren robbery. Carpenter's counsel then asked Foster whether he remembered "saying something different" to Ruiz. Foster said that he did not. That answer did not show that Foster's memory needed refreshing; it showed that Foster disagreed with Carpenter about what Foster had told Ruiz. What Carpenter actually sought to do with the report was not refresh Ruiz's memory, but impeach his testimony. The district court did not abuse its discretion in ruling that Carpenter could not use the report for that purpose.

To the same end, Carpenter argues that the district court should have allowed him to introduce Ruiz's report as extrinsic evidence of a prior inconsistent statement under Federal Rule of Evidence 613(b). But an FBI agent's written summary of an interview with a declarant cannot be used to impeach the declarant's later testimony unless the declarant has attested to the report's accuracy. *See United States v. Barile*, 286 F.3d 749, 757 (4th Cir. 2002); *United States v. Schoenborn*, 4 F.3d 1424, 1429 & n.3 (7th Cir. 1993). Foster has not done that here; to the contrary, Foster testified that Ruiz's report would have been wrong if it said that Sanders rather than Carpenter had told him about the plans for the Warren robbery. The district court thus correctly

barred the report's introduction at trial.

C.

1.

Carpenter's remaining argument is that his 1,395-month sentence is so disproportionate to his crimes as to violate the Eighth Amendment's prohibition on cruel and unusual punishment. He also argues that his mandatory-minimum sentences for his § 924(c) convictions violate the constitutional separation of powers. We consider both issues de novo. *See United States v. Kelsor*, 665 F.3d 684, 701 (6th Cir. 2011).

"[O]nly an extreme disparity between crime and sentence offends the Eighth Amendment." *United States v. Odeneal*, 517 F.3d 406, 414 (6th Cir. 2008). In *Solem v. Helm*, 463 U.S. 277 (1983), the Supreme Court held that the Eighth Amendment prohibited a state court from sentencing to life imprisonment without parole a recidivist criminal who wrote a bad check for $100. But in *Ewing v. California*, 538 U.S. 11 (2003), the Supreme Court rejected the Eighth Amendment claim of a defendant who was sentenced to 25 years to life for stealing several golf clubs. 538 U.S. at 28-30.

Carpenter has a long criminal history. In this case, as the district court observed, Carpenter organized and led several "very violent" robberies that put his victims "in extreme danger[.]" Meanwhile, in other armed-robbery cases, we have already held that sentences even longer than Carpenter's were constitutionally permissible. *See United States v. Clark*, 634 F.3d 874, 877-78

(6th Cir. 2011) (2,269 months); *United States v. Watkins*, 509 F.3d 277, 282 (6th Cir. 2007) (1,772 months). Carpenter's sentence does not violate the Eighth Amendment.

Nor do his mandatory-minimum sentences violate the constitutional separation of powers. "Congress has the power to define criminal punishments without giving the courts any sentencing discretion." *Chapman v. United States*, 500 U.S. 453, 467 (1991). Carpenter acknowledges that we have "flatly rejected" his argument in other cases. Carpenter Br. at 54; *see, e.g., United States v. Cecil*, 615 F.3d 678, 696 (6th Cir. 2010). This case is no different.

2.

Sanders challenges his sentence on non-constitutional grounds, arguing that the district court misapplied the Sentencing Guidelines and that his sentence is "greater than necessary" to accomplish the remedial objectives of incarceration. *See* 18 U.S.C. § 3553. We review for clear error the district court's factual findings in support of Sanders's sentence, and review the sentence itself for an abuse of discretion. *See United States v. Randolph*, 794 F.3d 602, 614 (6th Cir. 2015).

Sanders argues first that the district court incorrectly applied sentencing enhancements for brandishing or possessing a firearm in furtherance of robbery, and for physically restraining a person in furtherance of a robbery. *See* U.S.S.G. §§ 2B3.1(b)(2)(C), (b)(4)(B). Sanders himself need not have committed those acts in order for the enhancements to apply; rather, he need only have

known it was "reasonably probable" that a co-participant would commit them. *See United States v. Woods*, 604 F.3d 286, 291 (6th Cir. 2010).

That standard is met here. During the January 7, 2011 robbery, Sanders's accomplice Juston Young returned to the getaway car with gun in hand. Thus, when Sanders teamed up with Young and others for another robbery on March 4, Sanders could have easily foreseen that Young would brandish a firearm in the course of the crime—as in fact Young did. The district court did not clearly err in finding that the firearm enhancement applied to Sanders.

Nor did the court err in finding that Sanders could foresee that Young would physically restrain someone during the March 4 robbery. As a general matter, an accomplice to robbery should foresee that robbery likely entails physical restraint or worse. *See* U.S. Sentencing Guidelines Manual § 1B1.3 cmt. n.2 (2012). And Sanders knew specifically that the plan for that robbery was for the robbers to move customers and employees to the back of the store. The physical-restraint enhancement was therefore proper. That leaves an enhancement for brandishing a firearm during the January 7 robbery. But that enhancement had no effect on Sanders's Guidelines range: the offense level for the March 4 robbery was higher than the offense level for the January 7 robbery, even with the brandishing enhancement; and the offense level for the March 4 robbery, not the January 7 one, thus determined his total offense level under the Guidelines. Any error as to the brandishing enhancement for the January 7 robbery was

therefore harmless. *See United States v. Jeross*, 521 F.3d 562, 574-76 (6th Cir. 2008).

Finally, the district court acted within its discretion in sentencing Sanders to 170 months' imprisonment, which fell squarely within his Guidelines range of 151 to 188 months. Within-Guidelines sentences are presumptively reasonable in this circuit. *See United States v. Kamper*, 748 F.3d 728, 739-40 (6th Cir. 2014). Moreover, the district court considered and rejected the arguments that Sanders raised at his sentencing hearing, and otherwise properly determined that the sentence was appropriate in light of 18 U.S.C. § 3553(a). The court did not abuse its discretion.

* * *

The judgments in both cases are affirmed.

CONCURRENCE

STRANCH, Circuit Judge, concurring. I join Parts II.B and III of the majority opinion, which resolve Carpenter's and Sanders's statutory, evidentiary, and sentencing claims. I concur only in the judgment with respect to Part II.A because I believe that the sheer quantity of sensitive information procured without a warrant in this case raises Fourth Amendment concerns of the type the Supreme Court and our circuit acknowledged in *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring), and in *United States v. Skinner*, 690 F.3d 772, 780 (6th Cir. 2012). Though

I write to address those concerns, particularly the nature of the tests we apply in this rapidly changing area of technology. I find it unnecessary to reach a definitive conclusion on the Fourth Amendment issue. I concur with the majority on the basis that were there a Fourth Amendment violation, I would hold that the district court's denial of Carpenter and Sanders's motion to suppress was nevertheless proper because some extension of the good-faith exception to the exclusionary rule would be appropriate.

A. Fourth Amendment Concerns

At issue here is not whether the cell-site location information (CSLI) for Carpenter and Sanders could have been obtained under the Stored Communications Act (SCA). The question is whether it should have been sought through provisions of the SCA directing the government to obtain a warrant with a probable cause showing, 18 U.S.C. § 2703(c)(1)(A), or a court order based on the specified "reasonable grounds[,]" *id.* §§ 2703(c)(1)(B), (d). This leads us to the requirements of the Fourth Amendment.

Fourth Amendment law was complicated in the time of paper correspondence and land phone lines. The addition of cellular (not to mention internet) communication has left courts struggling to determine if (and how) existing tests apply or whether new tests should be framed. I am inclined to favor the latter approach for several reasons, particularly one suggested by Justice Sotomayor: "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of

privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citations omitted).

It is easier to see why the existing tests present problems than it is to articulate a test that will not. This difficulty is exemplified by the two conceptual categories under the Fourth Amendment found in this case and the law that governs each. The majority accurately describes two different strains of law, one addressing the distinction between GPS tracking and the less accurate CSLI obtained and used in this case and the other "between the content of a communication and the information necessary to convey it." (Majority Op. at 2.) To understand whether and how the tests established in these two different strains of Fourth Amendment law might apply requires a brief review of each.

First, the distinction between GPS tracking and CSLI acquisition. CSLI does appear to provide significantly less precise information about a person's whereabouts than GPS and, consequently, I agree that a person's privacy interest in the CSLI his or her cell phone generates may indeed be lesser. *See, e.g.*, *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."); *id.* at 963 (Alito,

J., concurring) ("For older phones, the accuracy of the location information depends on the density of the tower network, but new 'smart phones,' which are equipped with a GPS device, permit more precise tracking.").

But precision is not the only variable with legal significance. In *United States v. Skinner*, we addressed the government's use of GPS data emitted by a suspect's cell phone to track the suspect's whereabouts over the course of three days. *Skinner*, 690 F.3d at 774–76. The tracking took place pursuant to a court order authorizing the suspect's phone company to provide the government access to the GPS data emitted by the suspect's pay-as-you-go cell phone. *See id.* at 776. The majority opinion there acknowledged "the concern raised by Justice Alito's concurrence in *Jones*" that long-term location monitoring in government investigations impinges on expectations of privacy, but held that the concern was not implicated in Skinner's case because of the relatively short tracking period. *Id.* at 780. It distinguished *Jones*, explaining that "[w]hile *Jones* involved intensive monitoring over a 28-day period, here the DEA agents only tracked Skinner's cell phone for three days. Such 'relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.'" *Id.* (quoting *Jones*, 132 S. Ct. at 964 (Alito, J., concurring)). But *Skinner* framed this conclusion with a key caveat: "There may be situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." *Id.*

Primarily analyzing this case under the tests established for the assertion of a privacy interest in business records, the majority here determines that the CSLI is unprotected because it deals with routing or conveying information, not the content of the related communications. (Majority Op. at 6–8.) This analysis reflects a valid distinction in that arena of the law. It is here, however, that my concern arises with the existing tests. It seems to me that our case resides at the intersection of the law governing tracking of personal location and the law governing privacy interests in business records. This case involves tracking physical location through cell towers and a personal phone, a device routinely carried on the individual's person; it also involves the compelled provision of records that reflect such tracking. In light of the personal tracking concerns articulated in our precedent, I am not convinced that the situation before us can be addressed appropriately with a test primarily used to obtain business records such as credit card purchases –records that do not necessarily reflect personal location. And it seems to me that the business records test is ill suited to address the issues regarding personal location that are before us. I therefore return to the law governing location.

I begin by acknowledging that this case involves CSLI that does not reach the specificity of GPS. Nonetheless, *Skinner* recognizes "situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." *Skinner*, 690 F.3d at 780. The tracking of cell-phone data in this case went far beyond 3 or even

28 days—the government procured approximately 127 days of CSLI records for Carpenter and 88 days for Sanders. That is close to four and three months, respectively. Even taking into account the less precise nature of CSLI as compared to GPS, such extensive monitoring far exceeds the threshold we identified in *Skinner* and the warrantless acquisition of such substantial quantities of CSLI implicates the *Skinner*/*Jones* concerns. I do not think that treating the CSLI obtained as a "business record" and applying that test addresses our circuit's stated concern regarding long-term, comprehensive tracking of an individual's location without a warrant. At issue here is neither relatively innocuous routing information nor precise GPS locator information: it is personal location information that partakes of both. I am also concerned about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled. I conclude that our precedent suggests the need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances.

B. The Exclusionary Rule & Good-Faith Exception

"When evidence is obtained in violation of the Fourth Amendment, the judicially developed exclusionary rule usually precludes its use in a criminal proceeding against the victim of the illegal search and seizure." *Illinois v. Krull*, 480 U.S. 340, 347 (1987). The exclusionary rule is not intended "to redress the injury to the privacy of the search victim[.] . . . Instead, the rule's prime purpose is to

Primarily analyzing this case under the tests established for the assertion of a privacy interest in business records, the majority here determines that the CSLI is unprotected because it deals with routing or conveying information, not the content of the related communications. (Majority Op. at 6–8.) This analysis reflects a valid distinction in that arena of the law. It is here, however, that my concern arises with the existing tests. It seems to me that our case resides at the intersection of the law governing tracking of personal location and the law governing privacy interests in business records. This case involves tracking physical location through cell towers and a personal phone, a device routinely carried on the individual's person; it also involves the compelled provision of records that reflect such tracking. In light of the personal tracking concerns articulated in our precedent, I am not convinced that the situation before us can be addressed appropriately with a test primarily used to obtain business records such as credit card purchases—records that do not necessarily reflect personal location. And it seems to me that the business records test is ill suited to address the issues regarding personal location that are before us. I therefore return to the law governing location.

I begin by acknowledging that this case involves CSLI that does not reach the specificity of GPS. Nonetheless, *Skinner* recognizes "situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." *Skinner*, 690 F.3d at 780. The tracking of cell-phone data in this case went far beyond 3 or even

28 days—the government procured approximately 127 days of CSLI records for Carpenter and 88 days for Sanders. That is close to four and three months, respectively. Even taking into account the less precise nature of CSLI as compared to GPS, such extensive monitoring far exceeds the threshold we identified in *Skinner* and the warrantless acquisition of such substantial quantities of CSLI implicates the *Skinner*/*Jones* concerns. I do not think that treating the CSLI obtained as a "business record" and applying that test addresses our circuit's stated concern regarding long-term, comprehensive tracking of an individual's location without a warrant. At issue here is neither relatively innocuous routing information nor precise GPS locator information: it is personal location information that partakes of both. I am also concerned about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled. I conclude that our precedent suggests the need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances.

B. The Exclusionary Rule & Good-Faith Exception

"When evidence is obtained in violation of the Fourth Amendment, the judicially developed exclusionary rule usually precludes its use in a criminal proceeding against the victim of the illegal search and seizure." *Illinois* v. *Krull*, 480 U.S. 340, 347 (1987). The exclusionary rule is not intended "to redress the injury to the privacy of the search victim[.] . . . Instead, the rule's prime purpose is to

deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures[.]" *United States v. Calandra*, 414 U.S. 338, 347 (1974). "As with any remedial device, application of the exclusionary rule properly has been restricted to those situations in which its remedial purpose is effectively advanced." *Krull*, 480 U.S. at 347.

This restriction has led the Supreme Court to articulate certain "exceptions" to the exclusionary rule. For example, in *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court held that courts generally should not apply the exclusionary rule to evidence obtained by police officers whose reliance on a search warrant issued by a neutral magistrate was objectively reasonable, even if the warrant was ultimately found to be defective. *See Leon*, 468 U.S. at 905– 26; *see also id.* at 926 ("In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause."). The Court explained that "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope[,]" "[p]enalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Id.* at 920–21 (footnote omitted). In *Illinois v. Krull*, the Supreme Court extended the good-faith exception articulated in *Leon* to evidence obtained in reasonable reliance on a statute that is subsequently declared

unconstitutional, reasoning "that the greatest deterrent to the enactment of unconstitutional statutes by a legislature is the power of the courts to invalidate such statutes." *Krull*, 480 U.S. at 352; *see also id.* at 349–350.

In the instant case, there is nothing to suggest that the FBI agents who obtained the CSLI of Carpenter and Sanders pursuant to the SCA engaged in any intentional misconduct. Suppressing the CSLI at trial would not have the requisite deterrent effect on future unlawful conduct and application of the exclusionary rule is therefore inappropriate. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 333–34 (6th Cir. 2010) (Keith, J., concurring). Assuming without deciding that this situation states a Fourth Amendment violation, I would still affirm the district court's denial of Carpenter and Sanders's motion to suppress on this ground.

C. Judicial Review

One further issue of importance bears mentioning. The majority may be correct that Congress is well positioned to gauge changing public attitudes toward new and evolving technology. This institutional advantage may even weigh in favor of approaching challenges to statutes that balance privacy and public safety interests with some caution. But I do not see this case primarily as a challenge to the constitutionality of the SCA's provisions that authorize the government to seek secured communications through *either* an order *or* a warrant. The question before us is one that courts routinely answer: did the search at issue require a

warrant? That the government sought and obtained an order under the SCA does not immunize that order from challenge on Fourth Amendment grounds. As relevant here, our circuit has already had occasion to weigh the propriety of an order under the SCA and to have found that order wanting. *Warshak* explained that "to the extent that the SCA purports to permit the government to obtain [a subscriber's] emails [from an internet service provider] warrantlessly, the SCA is unconstitutional." *Id.* at 288. I do not read that holding as declaring the balance struck by the SCA unconstitutional. (*See* Majority Op. at 10–11.) *Warshak* simply found that one proposed interpretation or use of the SCA as applied did not comply with the Fourth Amendment's requirement for a warrant based on probable cause. Determining the parameters of the Fourth Amendment is the task of the judiciary. *See United States v. Windsor*, 133 S. Ct. 2675, 2688 (2013) (quoting *Zivotofsky v. Clinton*, 132 S. Ct. 1421, 1427 (2012)). The runaway pace of technological development makes this task more difficult. But the job is ours nonetheless and the circumstances before us lead me to believe that we have more work to do to determine the best methods for assessing the application of the Fourth Amendment in the context of new technology.

No. 14-1572

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

FILED
Jun 29, 2016
Deborah S. Hunt, Clerk

v.

ORDER

TIMOTHY IVORY-CARPENTER,

Defendant-Appellant.

BEFORE: GUY, KETHLEDGE, and STRANCH, Circuit Judges.

The court received a petition for rehearing en banc. The original panel has reviewed the petition for rehearing and concludes that the issues raised in the petition were fully considered upon the original submission and decision of the case. The petition then was circulated to the full court. No judge has requested a vote on the suggestion for rehearing en banc.

Therefore, the petition is denied.

ENTERED BY ORDER OF THE COURT

Deborah S. Hunt, Clerk

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

United States of America,

Plaintiff,

v.

Criminal Case No. 12-20218
Honorable Sean F. Cox

Timothy Ivory Carpenter D-4 and
Timothy Michael Sanders D-11,

Defendants.
_____/

OPINION & ORDER

In this action, multiple Defendants were charged with various counts stemming from a series of robberies at cellular telephone stores. Defendants Timothy Carpenter ("Carpenter") and Timothy Sanders ("Sanders") are proceeding to trial. Defendants have filed the following two motions in limine that are contested by the Government: 1) a motion seeking to suppress cell phone data, as violative of the Fourth Amendment; and 2) a motion seeking to preclude Special Agent Christopher Hess from testifying as an expert witness at trial. As explained in greater detail below, the Court shall DENY both motions.

BACKGROUND

In this action, multiple Defendants were charged with various counts stemming from a series of robberies at cellular telephone stores. Defendants Carpenter and Sanders are proceeding to trial.

The Government does not contend that either Carpenter or Sanders entered the stores during the robberies. Rather, it contends that they "acted as lookouts, getaway drivers, planners and the like." (Govt.'s Trial Br. at 2). One of the robberies occurred in Warren Ohio, while the other six robberies occurred in the Metropolitan Detroit area.

The robberies that will be at issue at trial are those charged in Counts One through Fourteen, which occurred during the time period from December 13, 2010 to December 1, 2012.

On May 2, 2011, and again on June 7, 2011, the Government applied for and obtained court orders under 18 U.S.C. § 2703 for toll records, call detail records, and cell/site section information for several different cell phone numbers, including (313) 579-8507 and (313) 412-6845. (*See* 6/7/11 Order signed by Judge Stephen Murphy, D.E. No. 196-2; 5/2/11 Order signed by Magistrate Judge Michaelson, D.E. No. 221-3). Those Orders state that the Government had "demonstrated to the Court that there are *reasonable grounds to believe* that the information sought is relevant and material to a legitimate law enforcement investigation into possible violations of Title 18, United States Code, § 1951." (*Id.* at 1) (emphasis added).

At trial, the Government intends to present evidence through F.B.I. Special Agent Christopher Hess that, on March 4, 2011, Sanders's cell phone, (313) 579-8507, was located in a geographic area consistent with the robbery charged in Count 7, which occurred in Warren, Ohio. It also intends to present evidence that Carpenter's cell phone, (313) 412-6845, was in various areas consistent with

robberies charged in other Counts.

ANALYSIS

I. Motion to Suppress Cell Phone Data: D.E. 196 (With Joinder in D.E. 214)

In this motion, Defendant Sanders asks the Court to suppress cell phone data for cell phone number (313) 579-8507 because the data was obtained in violation of the Fourth Amendment. He makes two arguments. First, he argues that the "reasonable grounds standard" in the Stored Communications Act, 18 U.S.C. § 2703 *et seq.* ("the Act") is unconstitutional. Second, he argues that the Government did not present sufficient "reasonable grounds" information in order to obtain the order in any event.

Defendant Carpenter filed a "Notice of Joinder" (D.E. No. 214), wherein he stated that he "adopts and joins in Defendant [Sanders's] Motion in Limine To Suppress Cell Phone Data (R196)." In a supplement to that notice, he states that "[e]xcept for the difference in phone numbers referred to in the Order," the same analysis applies. (D.E. No. 216).

A. Should The Data Be Suppressed Because The "Reasonable Grounds Standard" In The Act Unconstitutional?

The parties agree that, under the Act, the standard of proof required for the Court Orders at issue here is as follows:

> (d) Requirements for court order . . . A court order for disclosure . . . shall issue

> only if the governmental entity offers specific and articulable facts showing that there are *reasonable grounds to believe* that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (emphasis added).

Defendants argue that the reasonable grounds standard in the Act is unconstitutional because a cell phone user has a reasonable expectation of privacy in prolonged surveillance data and therefore a probable cause determination should be required. Defendants claim that the Sixth Circuit has not addressed this issue and that lower courts that have addressed the issue have been divided. They rely on: 1) *In re U.S. for Historical Cell Site Data*, 747 F.Supp.2d 827 (S.D. Tex. 2010), wherein the district court held that the warrantless seizure of cell cite records over a period of two months was unreasonable because the phone user has a reasonable expectation of privacy in prolonged surveillance information); and 2) *In re Application of U.S.*, 736 F.Supp.2d 578 (E.D. N.Y. 2010), wherein the district court also held that historical cell site data is protected by the Fourth Amendment. Those district court judges were influenced by case law holding that placing a G.P.S. tracking device on a vehicle requires a warrant.

Sanders's brief, filed on November 21, 2013, indicates that the appeal in *In re Application of U.S.* is still pending (*see* Sanders's Br. at 5), but that is not the case. On July 30, 2013, the Fifth Circuit issued its decision *reversing the lower court's ruling*.

In response to Defendants' motion, the Government notes that Defendants have not directed the Court to a single decision by any United States Court of Appeals, much less the Sixth Circuit, that supports their position. The Government directs the Court to *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012).[1] In that case, the authorities obtained court orders for subscriber information, cell cite information, G.P.S. real-time location, and "ping" data for cell phones. *Id.* at 776. In affirming the district court's ruling denying the defendant's motion to suppress, the Sixth Circuit held that there was "no Fourth Amendment violation because [the defendant] did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone." *Id.* at 777. The *Skinner* court reaffirmed there is no legitimate expectation of privacy in cell site data because the "'cell-site data is simply a proxy'" for the defendant's visually observable location, and a defendant has no legitimate expectation of privacy in his movements along public highways. *Id.* at 779 (quoting *United States v. Forrest*, 355 F.3d 942, 951-52 (6th Cir. 2004)). The *Skinner* decision reflects that the Sixth Circuit views obtaining routine cell phone data quite differently than it does data obtained via a G.P.S. device being placed on a vehicle without a warrant:

---

[1] The Government also contends that if Section 2703(d) were found unconstitutional in this case, the evidence should not be suppressed in any event because the agents relied in good faith on the Act in obtaining the evidence. (Govt.'s Br. at 5) (citing *United States v. Warshak*, 631 F.3d 266, 288-89 (6th Cir. 2010)). The Court agrees that this is an additional basis for denying the motion.

> When criminals use modern technological devices to carry out criminal acts . . . they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them. *This is not a case in which the government secretly placed a tracking device in someone's car.*

Id. at 774 (emphasis added).

This Court rejects Defendants' argument that the Act is unconstitutional.

B. Did The Government Present Sufficient Reasonable Grounds?

In this motion, Defendants also make a secondary argument that the Government did not present sufficient reasonable grounds to obtain the orders in any event. (*See* Sanders's Br. at 2, asserting that, "upon information and belief," the order was "obtained in violation of the Act because 'reasonable grounds' were not presented to obtain the Order.").

In response, the Government contends it satisfied the applicable standard. (*See* Govt.'s Br. at 5-6). The Court agrees.

The Order that Sanders challenges is the one issued by Judge Murphy. The Application that requested that order (D.E. No. 221-2) set forth the factual basis for the Government's request and included, among other things, that: 1) there was an ongoing criminal investigation as to a series of armed robberies at Radio Shack and T-Mobile stores in Detroit, Michigan; 2) the Detroit Police Department

has arrested four individuals believed to be involved in the robberies; 3) a cooperating defendant was interviewed, admitted his role as to nine robberies, identified others involved in the robberies, indicated they planned to do additional robberies, and provided his own cell phone number and those of others involved in the robberies; and 4) the cell site records are needed to assist in identifying and locating the other persons involved in the robberies. The application that requested the order challenged by Carpenter is nearly identical. The Court finds that the Applications were supported by specific and articulable facts, and therefore meets the "diminished standard that applies to § 2703(d) applications." *United States v. Warshak*, 631 F.3d 266, 291 (6th Cir. 2010).

Accordingly, the Court shall deny this motion.

II. Motion To Exclude Lay And Expert Testimony: D.E. 211 (Joinder In D.E. 215)

In this motion, filed by Carpenter and joined by Sanders, Defendants ask the Court to enter an order excluding expert testimony regarding the operation of cell towers (i.e., the testimony of Special Agent Hess). They ask the Court to do so on several grounds, which are addressed below.

A. Should The Court Exclude Hess's Report Because It Is Untimely, Unfairly Prejudicial, And Fails To Meet Rule 16 Requirements?

First, Defendants argue that the untimely production of Special Agent Hess's report is unfairly prejudicial and fails to meet the requirements of Fed.

R. Crim. P. 16. (Def.'s Br. at 3). Carpenter asserts that he received the discovery which relates to the testimony of Hess "just three weeks before trial." He contends the tardiness of the report is prejudicial because the subject matter (cell-site analysis) is specialized information and the "last-minute disclosure by the Government leaves the Defendant without the tools to effectively cross-examine SA Hess." (*Id.* at 4). Carpenter also contends that Hess's report is deficient because it does sufficiently explain the bases and reasons for his opinions.

As the Government details in its Response Brief, Defense Counsel has been aware for *at least several months prior to trial* that the Government would seek to present an expert witness in cell-site analysis at trial:

1) On April 15, 2013, the Government filed a Discovery Notice (D.E. No. 89) advising Carpenter that it "intends to introduce at trial testimony from one or more experts in the following areas of expertise: cell tower location analysis" and referencing evidence involving "telephone call records and location data." (*Id.*) (underlining in original);

2) On August 16, 3023, the Government filed an identical notice as to Sanders. (D.E. No. 150);

3) During a Status Conference on October 28, 2013, Defense Counsel stated that they needed Special Agent Hess's report in sufficient time that they could hire their own experts. The Court advised Defense Counsel of the recent case that Judge Borman had involving Hess, wherein another expert was called to rebut his

testimony. On that same day, the Court ordered the Government to provide Defense Counsel with Hess's report no later than November 7, 2013.

4) Neither Defendant filed a motion seeking the report earlier or asking the Court to adjourn the trial date.

5) The Government contends that it met the Court's deadline for providing Hess's report; and

6) On November 22, 2013, Sanders submitted a witness list that identifies his own expert witness, Ryan J. Harmon. Carpenter joined in that witness list.

The Court rejects Defendants' timeliness and unfair prejudice argument based on timeliness arguments.

Defendants also contend that Hess's report does not provide sufficient information as to the bases and reasons for his opinions. That argument is also rejected. Hess's report contains a section titled, "Basic Principals [sic] Utilized In Record Analysis" that explains the underlying technology and how it works. Hess then applied those principles and opined that Defendants were in geographic areas consistent with certain robberies.

B. Should The Court Preclude Hess's Proposed Expert Testimony Under Fed. R. Evid. 702 And *Daubert*?

Next, Defendants ask this Court to preclude the Government from calling Special Agent Hess as an expert at trial, pursuant to Fed. R. Evid. 702 and

Daubert, because his proposed testimony is not sufficiently reliable to qualify as expert testimony.

"District court judges must determine whether an expert's testimony is both relevant and reliable when ruling on its admission." *Clay v. Ford Motor Company*, 215 F.3d 663, 667 (6th Cir. 2000). A trial judge's determinations regarding the admissibility of expert testimony are guided by Fed. R. Evid. 702 and *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

Rule 702 of the Federal Rules of Evidence governs testimony by experts and provides as follows:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
> (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
> (b) the testimony is based on sufficient facts or data;
> (c) the testimony is the product of reliable principles and methods; and
> (d) the expert has reliably applied the principles and methods to the facts of the case.

Fed. R. Evid. 702.

Under *Daubert*, the trial court acts as a "gatekeeper" that ensures that any and all scientific testimony or evidence admitted is not only relevant, but reliable. *Daubert* sets forth a nonexclusive list of

factors relevant to this inquiry: 1) whether the theory or technique can be or has been tested; 2) whether it has been subjected to peer review; 3) whether there is a known or potential rate of error; and 4) whether the theory or technique enjoys general acceptance in the relevant scientific community. *Daubert*, 509 U.S at 593-94. In *Kumho Tire Co. v. Carmichael*, 526 U.S. 137 (1999), the Supreme Court confirmed that "the general gatekeeping obligation set forth in *Daubert*" "applies when considering all expert testimony, including testimony based on technical and other specialized knowledge." *Clay v. Ford Motor Co.*, 215 F.3d at 667. "It further held that the specific *Daubert* factors – testing, peer review and publication, potential rate of error, and general acceptance in the relevant community – may be considered by the district court even when the proffered expert testimony is not scientific." *Id.* Whether these specific factors are reasonable measures of reliability in a particular case is a matter that the law grants the trial judge broad latitude to determine. *Id.*

"It is the proponent of the testimony that must establish its admissibility by a preponderance of proof." *Nelson v. Tennessee Gas Pipeline Co.*, 243 F.3d 244, 251 (6th Cir. 2001) (citing *Daubert*, 509 U.S. at 592 n.10)).

A district court is not obligated to hold a *Daubert* hearing (*see Clay v. Ford Motor Company*, 215 F.3d at 667; *Nelson*, 243 F.3d at 249) and this Court declines to do so here. A *Daubert* hearing is unnecessary in light of the full briefing of the issues by the parties and the materials submitted to date.

1. The Proposed Expert Testimony Is Relevant

Here, Defendants do not appear to dispute that Hess's proposed testimony is relevant. And even if they did, the Court concludes that his testimony is relevant.

"Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." Fed. R. Civ. P. 401.

The proposed expert testimony is that, during the relevant times during which certain robberies occurred, call activity from Defendants' cell phones place them in the general area of the stores where the robberies took place. Such testimony is relevant because it makes a fact of consequence in determining the action (whether Defendants were physically present near the stores on the dates and times of the robberies) more probable than it would be without the evidence. Accordingly, the Court finds that Special Agent Hess's specialized knowledge will help the trier of fact to understand the evidence and to determine a fact in issue in this case. At trial, however, a proper foundation will have to be established regarding the cell phones at issue before Special Agent Hess can testify.

2. The Proposed Expert Testimony Is Sufficiently Reliable.

The Government's Brief indicates that Special Agent Hess has testified as an expert in cell site analysis in over 25 criminal trials, including four cases in this district. Indeed, Special Agent Hess

recently testified as an expert witness in another criminal trial before this Court, *United States v. Reynolds*. *See United States v. Reynolds*, 2013 WL 2480684 (E.D. Mich. June 10, 2013).

In *Reynolds*, the defendant did not argue that Special Agent Hess is not qualified as an expert in the area of cell site analysis. Rather, he argued that cell site analysis should not be permitted because it is not sufficiently reliable because: 1) the testimony is based upon an unreliable methodology for the purpose for which it is offered; and 2) historical cell site analysis is inadmissible to establish a specific location. Both of those arguments were premised on the assumption that the Government was going to have Special Agent Hess testify using cell site analysis to opine that Defendant was present at a *specific location* on the relevant dates and times.

In this case, the Government only seeks to have Hess testify that Defendants' cell phones were in geographic areas "consistent with" the locations where the robberies occurred.

Testimony about cellular phone technology and the ability to determine the general area where calls are placed and received has been widely accepted by federal courts. *See e.g.*, *United States v. Weathers*, 169 F.3d 336, 339 (6th Cir. 1999); *United States v. Schaffer*, 439 Fed. App'x 344, 347 (5th Cir. 2011); *United States v. Jones*,___F.2d___, 2013 WL 246615 (D.D.C. 2013); *United States v. Benford*, 2010 WL 2346305 (N.D. Ind. 2010); *United States v. Allums*, 2009 WL 806748 (D. Utah 2009). This Court again concludes that Special Agent Hess's proposed testimony is the product of reliable principles and methods and he has reliably applied those principles

and methods to the facts of this case.

Moreover, Defense Counsel have indicated that Defendants may call their own expert witness, to challenge the opinions of Special Agent Hess and provide opinion testimony regarding the locations of the cell phones at issue during the relevant time periods.

The weight to be afforded any expert witness testimony presented at trial can be determined by the jury.

The Court shall therefore deny without prejudice Defendants' motion seeking to preclude the expert testimony of Special Agent Hess and shall rule that although Special Agent Hess's proposed testimony regarding cell site analysis is both relevant and reliable, that the Government must lay an appropriate foundation before Special Agent Hess may testify at trial.

CONCLUSION & ORDER

For the reasons set forth above, IT IS ORDERED that Defendants' Motion seeking to Suppress Cell Phone Data (D.E. Nos. 196 & 214) IS DENIED.

IT IS FURTHER ORDERED that the Court DENIES WITHOUT PREJUDICE Defendants' motion seeking to preclude the expert testimony of Special Agent Hess (D.E. Nos. 211 and 215) and RULES that although Special Agent Hess's proposed testimony regarding cell site analysis is both relevant and reliable, the Government must lay an appropriate foundation before Special Agent Hess may testify at trial.

IT IS SO ORDERED.

S/Sean F. Cox

Sean F. Cox

United States District Judge

Dated: December 6, 2013

I hereby certify that a copy of the foregoing document was served upon counsel of record on December 6, 2013, by electronic and/or ordinary mail.

S/Jennifer McCoy

Case Manager

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER FOR DISCLOSURE OF TELECOMMUNICATIONS RECORDS /

Case: 2:11-us-60044A
Judge: Murphy Stephen J.
PEN: Sealed Matter (jj)

APPLICATION

NOW COMES the United States of America, by and through its attorneys, Barbara L. McQuade, United States Attorney, and John N. O'Brien, Assistant United States Attorney, and pursuant to Title 18 United States Code, Section 2703(c) and (d), requests that this Honorable Court issue an Order requiring that:

Adelphia Communications, Adelphia Long Distance, Airlink Wireless, Airvoice Wireless, Allegiance Telecom of California, Inc., AllTel Communications, Alltel Georgia Communications Corp, AllTel Telephone Services, American Cellular, American Paging, Ameritech Michigan, Arch Communications, Arch Paging Communications, Arch Wireless; Astound, AT&T Broadband, AT&T Local Service, AT&T Long Distance, AT&T Wireless Services, Bay Star Communications, Bell South Telecommunications, Bittell Communications, Bluegrass Cellular, Bullseye Telecom, Cavalier Business

Communications, Comcast Cable Communications, CCT Telecom, Cellco Partnership doing business as Verizon Wireless, Cellnet Communications, Cellular Information Systems of Florence, Cellular One, Cellular South, CellulPage, Central Telephone Company of Nevada doing business as Sprint of Nevada, Central Wireless Partnership doing business as Sprint PCS, Cincinnati Bell, Cingular Wireless, Comm South Companies, Commonwealth Communications, Competitive Communications, Inc., Comstat Mobile, Corecomm Limited Cox Communications, Cox Communications Arizona, Dobson Cellular, Crickett Communications, Inc., Cue Paging, DBS Communications, Dobson Communications, Duo County Telephone, Easton Telecomm Service; Edge Wireless LLC, Electric Lightwave, Embarq, Encompass Communications, Ernest Communications, Evans Telephone Company, Excel Communications, Excel Telecommunications, Focal Communications Corporation, Frontier: A Citizens Communications Company, Genesis Communications International, Global Crossing, GTE Paging, Granite Telecommunications, Hartington Telecommunications, Highland Telephone Co-op, ICG Communications, ICG Telecom Group, Iridium North America, ITC Deltacom, IXC Communications, J.D. Services, KMC Telecom, Leap Wireless, Level 3 Communications, Inc., Long Distance Management, Long Distance of Michigan, MCI-Worldcom, MCI-Worldcom Wireless, Metrocall, Metro PCS, M Power Communications, Nationwide Paging, Navigator

Telecommunications LLC, Network Telephone, Networkservices L.L.C., NII Communications, Inc., NSC Communications, O1 Communications, OCI Communications, Omega Services, LLC, One Communications, One Star Long Distance, Optel Texas, Inc. Pac West Telecommunications Incorporated, Pacific Bell, Paetec, Page Plus Communications, Pagemart, Phonetec, Qwest Communications, RCN Communications, Revol, Roseville Telephone Company, Sage Telecom, SBC Ameritech, SBC California, SBC Communications, SBC Nevada Bell, SBC Pacific Bell, SBC Southwestern Bell, Seren Innovations, SkyTel Nationwide, Source One Wireless, Southwestern Bell, Southwestern Bell Wireless, Sprint-Nextel Corporation, Sprint Communications, Sprint Long Distance, Sprint Spectrum L.P., TCG America, Inc., TDS Metrocom, Inc., Telenet Worldwide, Telepacific Communications, Telescape Communications, Teligent, Time-Warner Cable, Time-Warner Telecom, Tracfone Wireless, Inc., Transtel, Trinsic Communications, T-Mobile USA Inc., T-Mobile/Omnipoint, US Cellular, US TelePacific Corp doing business as TelePacific Communications, Variatee Wireless, Verizon California, Verizon District of Columbia, Verizon Maryland, Verizon New England, Verizon New Jersey, Verizon New York, Verizon Northwest, Verizon Texas, Verizon Wireless, Verizon Wireless Paging, Weblink Wireless, Virgin Mobile, VoiceStream Wireless, West Coast PCS LLC doing business as Sure West Wireless, Western Wireless Corporation, Wide Open West, Winstar Communications, WorldCom,

XO Communications, Xspedius Communications
(hereinafter the **telecommunication carriers**)

disclose and furnish the Federal Bureau of Investigation the transactional records described below which pertain to the following telephone numbers, hereafter referred to as "target telephones":

(313) 579-8503
T-Mobile

(313) 412-6845
(313) 424-9573
Metro PCS

(313) 622-0775
(313) 218-2477
(313) 695-9294
Sprint PCS

The transactional records requested include:

A. All subscriber information and toll records including listed and unlisted numbers dialed or otherwise transmitted to and from target telephones from December 1, 2010 to present. In addition, the listed providers are requested to disclose cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls, upon oral or written request by agents of the Federal Bureau of Investigation

B. Records, credit and billing records, can be reached numbers (CBR), custom calling features, and primary long distance carrier, and caller ID for the target telephones.

In support of this application, John N. O'Brien, Assistant United States Attorney states the following:

A. Applicant is an attorney for the government as defined in Rule 1(b)(1)(B) of the Federal Rules of Criminal Procedure and therefore, pursuant to Section 2703(c)(l) and 2703(d) of Title 18, United States Code, may apply for disclosure of telecommunications records.

B. Applicant certifies that based on information from Special Agent Vincente Ruiz of the Federal Bureau of Investigation there exists reasonable grounds to believe that the subscriber information and cell site information requested will be relevant and material to an ongoing criminal investigation. The facts supporting this conclusion include the following:

On April 6, 2011, officers from the Detroit Police Department arrested four individuals, believed to be involved in a series of armed robberies of Radio Shack and T-Mobile stores in Detroit, Michigan.

On April 26, 2011, a cooperating defendant was interviewed about his involvement in those armed robberies and admitted he had a role in eight different robberies that started in December of 2010 and lasted through March of 2011 at Radio Shack and T-Mobile stores in Michigan and Ohio. The defendant further admitted that others involved with the armed robberies were not taken into custody when he was arrested. The core members were usually the same three individuals, but they regularly brought in others to assist as getaway

drivers and look-outs. The defendant identified 15 other individuals who had been involved in at least one of the eight robberies. Four of those individuals had been involved in multiple armed robberies and one had been involved in at least six of the robberies. The defendant also stated that some of the individuals not in custody had been planning to rob more stores in Dayton, Ohio.

It is anticipated that the requested records will assist in identifying and locating the other individuals believed to be involved in the armed robberies.

Additionally, the requested telecommunications records should yield information that is relevant and material to corroborate surveillance information and may identify potential witnesses and/or targets. The requested information will therefore further the Federal Bureau of Investigation in their investigation and provide evidence that Timothy Sanders, Timothy Carpenter and other known and unknown individuals are violating provisions of Title 18, United States Code, §1951.

Applicant requests that the Court issue an Order pursuant to Title 18, United States Code, Section 2703(d) directing the **telecommunication carriers** to provide the requested records to agents of the Federal Bureau of Investigation

Applicant further requests that this application and Order be sealed by the Court until such time as the Court directs otherwise, since disclosure at this time would seriously jeopardize the investigation, and that the Court order the **telecommunication carriers** their agents and

employees not to disclose the existence of this Order or of this investigation to the subscriber, or to any other person unless otherwise directed by the Court.

Applicant further requests that this Court's Order apply not only to the telephone numbers listed above for the target telephone numbers, but also to any changed telephone number(s) subsequently assigned to an instrument bearing the same [ESN] [IMSI] [SIM] [IMEI][MSID][MIN] as the target telephone numbers, or any changed [ESN] [IMSI] [SIM] [IMEI] [MSID][MIN] subsequently assigned to the same telephone numbers as the target telephone numbers, or any additional changed telephone number(s) and or [ESN] [IMSI] [SIM] [IMEI] [MSID][MIN] listed to the same subscriber and/or wireless telephone accounts as the target telephone numbers within the period authorized by this Order.

WHEREFORE, it is respectfully requested that the Court grant an Order directing the **telecommunication carriers** to (1) provide the requested records to agents of the Federal Bureau of Investigation; (2) not to disclose the existence of this Order or the investigation to the subscriber or customer or to any unauthorized person unless or until ordered or authorized to do so by the court; and (3) sealing this application and accompanying Order.

Respectfully submitted,

Barbara L. McQuade
United States Attorney

MAY – 2 '06

John N. O'Brien
Assistant U.S. Attorney.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER FOR DISCLOSURE OF TELECOMMUNICATIONS RECORDS	Case: 2:11-us-60044A Judge: Murphy, Stephen J. PEN: Sealed Matter (jj)

ORDER

This matter, having come before the court pursuant to an application under Title 18, United States Code, Section 2703(d) by John N. O'Brien, an attorney for the Government, requesting the production of certain telecommunications records; the court finds that the applicant has certified and demonstrated to the Court that there are reasonable grounds to believe that the information sought is relevant and material to a legitimate law enforcement investigation into possible violations of Title 18, United States Code, §1951.

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d), that

Adelphia Communications, Adelphia Long Distance, Airlink Wireless, Airvoice Wireless, Allegiance Telecom of California, Inc., AllTel Communications, Alltel Georgia Communications Corp, AllTel Telephone Services, American Cellular, American Paging, Ameritech Michigan, Arch Communications, Arch Paging Commun-

ications, Arch Wireless; Astound, AT&T Broadband, AT&T Local Service, AT&T Long Distance, AT&T Wireless Services, Bay Star Communications, Bell South Telecommunications, Bittell Communications, Bluegrass Cellular, Bullseye Telecom, Cavalier Business Communications, Comcast Cable Communications, CCT Telecom, Cellco Partnership doing business as Verizon Wireless, Cellnet Communications, Cellular Information Systems of Florence, Cellular One, Cellular South, CelluPage, Central Telephone Company of Nevada doing business as Sprint of Nevada, Central Wireless Partnership doing business as Sprint PCS, Cincinnati Bell, Cingular Wireless, Comm South Companies, Commonwealth Communications, Competitive Communications, Inc., Comstat Mobile, Corecomm Limited Cox Communications, Cox Communications Arizona, Dobson Cellular, Crickett Communications, Inc., Cue Paging, DBS Communications, Dobson Communications, Duo County Telephone, Easton Telecomm Service; Edge Wireless LLC, Electric Lightwave, Embarq, Encompass Communications, Ernest Communications, Evans Telephone Company, Excel Communications, Excel Telecommunications, Focal Communications Corporation, Frontier: A Citizens Communications Company, Genesis Communications International, Global Crossing, GTE Paging, Granite Telecommunications, Hartington Telecommunications, Highland Telephone Co-op, ICG Communications, ICG Telecom Group, Iridium North America, ITC Deltacom, IXC Communications, J.D. Services,

KMC Telecom, Leap Wireless, Level 3 Communications, Inc., Long Distance Management, Long Distance of Michigan, MCI-Worldcom, MCI-Worldcom Wireless, Metrocall, Metro PCS, M Power Communications, Nationwide Paging, Navigator Telecommunications LLC, Network Telephone, Networkservices L.L.C., NII Communications, Inc., NSC Communications, O1 Communications, OCI Communications, Omega Services, LLC, One Communications, One Star Long Distance, Optel Texas, Inc. Pac West Telecommunications Incorporated, Pacific Bell, Paetec, Page Plus Communications, Pagemart, Phonetec, Qwest Communications, RCN Communications, Revol, Roseville Telephone Company, Sage Telecom, SBC Ameritech, SBC California, SBC Communications, SBC Nevada Bell, SBC Pacific Bell, SBC Southwestern Bell, Seren Innovations, SkyTel Nationwide, Source One Wireless, Southwestern Bell, Southwestern Bell Wireless, Sprint-Nextel Corporation, Sprint Communications, Sprint Long Distance, Sprint Spectrum L.P., TCG America, Inc., TDS Metrocom, Inc., Telenet Worldwide, Telepacific Communications, Telescape Communications, Teligent, Time-Warner Cable, Time-Warner Telecom, Tracfone Wireless, Inc., Transtel, Trinsic Communications, T-Mobile USA Inc., T-Mobile/Omnipoint, US Cellular, US TelePacific Corp doing business as TelePacific Communications, Variatec Wireless, Verizon California, Verizon District of Columbia, Verizon Maryland, Verizon New England, Verizon New Jersey, Verizon New York, Verizon Northwest,

Verizon Texas, Verizon Wireless, Verizon Wireless Paging, Weblink Wireless, Virgin Mobile, VoiceStream Wireless, West Coast PCS LLC doing business as Sure West Wireless, Western Wireless Corporation, Wide Open West, Winstar Communications, WorldCom, XO Communications, Xspedius Communications (hereinafter the **telecommunication carriers**)

disclose and furnish the Federal Bureau of Investigation the transactional records described below which pertain to the following telephone numbers, hereafter referred to as "target telephones":

(313) 579-8503
T-Mobile

(313) 412-6845
(313) 424-9573
Metro PCS

(313) 622-0775
(313) 218-2477
(313) 695-9294
Sprint PCS

The transactional records requested include:

A. All subscriber information and toll records including listed and unlisted numbers dialed or otherwise transmitted to and from target telephones from December 1, 2010 to present.

B. Records, credit and billing records, can be reached numbers (CBR), custom calling features, and primary long distance carrier, and caller ID for the target telephones.

IT IS FURTHER ORDERED pursuant to 18 U.S.C. Section 2703(c)(l)(B) and 2703(d), that the wireless carriers shall provide the locations of cell/site sector (physical addresses) for the target telephones at call origination and at call termination for incoming and outgoing calls during the relevant time period.

IT IS FURTHER ORDERED that this application and Order be sealed by the Court until such time as the Court directs otherwise, since disclosure at this time would seriously jeopardize the investigation; arid the Court orders that the **telecommunication carriers** their agents and employees not to disclose the existence of this Order or of this investigation to the subscriber, or to any other person unless otherwise directed by the Court.

IT IS FURTHER ORDERED that this authorization applies not only to the telephone numbers listed above for the target telephone numbers, but also to any changed telephone number(s) subsequently assigned to an instrument bearing the same [ESN][IMSI][SIM][IMEI][MSID] [MIN] as the target telephone numbers, or any changed [ESN][IMSI][SIM][IMEI][MSID][MIN] subsequently assigned to the same telephone numbers as the target telephone numbers, or any additional changed telephone number(s) and or [ESN][IMSI][SIM][IMEI][MSID][MIN] listed to the same subscriber and/or wireless telephone account as the target telephone numbers within the period authorized by this Order;

IT IS FURTHER ORDERED that the local, long distance and wireless carriers be compensated by the investigative agency for reasonable expenses incurred in providing technical assistance.

Honorable Laurie Michaelson
United States Magistrate Judge

Dated: 5/2/11

A True Copy
U. S. Attorney's Office
Eastern District of Michigan
BY: _____
Paralegal Specialist

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER FOR DISCLOSURE OF TELECOMMUNICATIONS RECORDS /	Tracking No.: 11US60044-C Hon. Stephen J. Murphy, III

APPLICATION

NOW COMES the United States of America, by and through its attorneys, Barbara L. McQuade, United States Attorney, and John N. O'Brien, Assistant United States Attorney, and pursuant to Title 18 United States Code, Section 2703(c) and (d), requests that this Honorable Court issue an Order requiring that:

Adelphia Communications, Adelphia Long Distance, Airlink Wireless, Airvoice Wireless, Allegiance Telecom of California, Inc., AllTel Communications, Alltel Georgia Communications Corp, AllTel Telephone Services, American Cellular, American Paging, Ameritech Michigan, Arch Communications, Arch Paging Communications, Arch Wireless; Astound, AT&T Broadband, AT&T Local Service, AT&T Long Distance, AT&T Wireless Services, Bay Star Communications, Bell South Telecommunications, Bittell Communications, Bluegrass Cellular, Bullseye Telecom, Cavalier Business

Communications, Comcast Cable Communications, CCT Telecom, Cellco Partnership doing business as Verizon Wireless, Cellnet Communications, Cellular Information Systems of Florence, Cellular One, Cellular South, CelluPage, Central Telephone Company of Nevada doing business as Sprint of Nevada, Central Wireless Partnership doing business as Sprint PCS, Cincinnati Bell, Cingular Wireless, Comm South Companies, Commonwealth Communications, Competitive Communications, Inc., Comstat Mobile, Corecomm Limited Cox Communications, Cox Communications Arizona, Dobson Cellular, Crickett Communications, Inc., Cue Paging, DBS Communications, Dobson Communications, Duo County Telephone, Easton Telecomm Service; Edge Wireless LLC, Electric Lightwave, Embarq, Encompass Communications, Ernest Communications, Evans Telephone Company, Excel Communications, Excel Telecommunications, Focal Communications Corporation, Frontier: A Citizens Communications Company, Genesis Communications International, Global Crossing, GTE Paging, Granite Telecommunications, Hartington Telecommunications, Highland Telephone Co-op, ICG Communications, ICG Telecom Group, Iridium North America, ITC Deltacom, IXC Communications, J.D. Services, KMC Telecom, Leap Wireless, Level 3 Communications, Inc., Long Distance Management, Long Distance of Michigan, MCI-Worldcom, MCI- Worldcom Wireless, Metrocall, Metro PCS, M Power Communications, Nationwide Paging, Navigator

Telecommunications LLC, Network Telephone, Networkservices L.L.C., NII Communications, Inc., NSC Communications, O1 Communications, OCI Communications, Omega Services, LLC, One Communications, One Star Long Distance, Optel Texas, Inc. Pac West Telecommunications Incorporated, Pacific Bell, Pactec, Page Plus Communications, Pagemart, Phonetec, Qwest Communications, RCN Communications, Revol, Roseville Telephone Company, Sage Telecom, SBC Ameritech, SBC California, SBCCommunications, SBC Nevada Bell, SBC Pacific Bell, SBC Southwestern Bell, Seren Innovations, SkyTel Nationwide, Source One Wireless, Southwestern Bell, Southwestern Bell Wireless, Sprint-Nextel Corporation, Sprint Communications, Sprint Long Distance, Sprint Spectrum L.P., TCG America, Inc., TDS Metrocom, Inc., Telenet Worldwide, Telepacific Communications, Telescape Communications, Teligent, Time-Warner Cable, Time-Warner Telecom, Tracfone Wireless, Inc., Transtel, Trinsic Communications, T-Mobile USA Inc., T-Mobile/Omnipoint, US Cellular, US TelePacific Corp doing business as TelePacific Communications, Variatee Wireless, Verizon California, Verizon District of Columbia, Verizon Maryland, Verizon New England, Verizon New Jersey, Verizon New York, Verizon Northwest, Verizon Texas, Verizon Wireless, Verizon Wireless Paging, Weblink Wireless, Virgin Mobile, VoiceStream Wireless, West Coast PCS LLC doing business as Sure West Wireless, Western Wireless Corporation, Wide Open West, Winstar Communications, WorldCom,

XO Communications, Xspedius Communications (hereinafter the **telecommunication carriers**)

disclose and furnish the Federal Bureau of Investigation the transactional records described below which pertain to the following telephone numbers, hereafter referred to as "target telephone":

(313) 412-6845
Metro PCS telephone number roaming on Sprint's cellular tower network

The transactional records requested include:

A. All subscriber information and toll records including listed and unlisted numbers dialed or otherwise transmitted to and from target telephones from March 1, 2011 to March 7, 2011, including roaming tower call detail records with cell site information. In addition, the listed providers are requested to disclose cell site information for the target telephone at call origination and at call termination for incoming and outgoing calls, upon oral or written request by agents of the Federal Bureau of Investigation.

B. Records, credit and billing records, can be reached numbers (CBR), custom calling features, and primary long distance carrier, and caller ID for the target telephone.

In support of this application, John N. O'Brien, Assistant United States Attorney states the following:

A. Applicant is an attorney for the government as defined in Rule 1(b)(1)(B) of the Federal Rules of Criminal Procedure and

therefore, pursuant to Section 2703(c)(l) and 2703(d) of Title 18, United States Code, may apply for disclosure of telecommunications records.

B. Applicant certifies that based on information from Special Agent Vincente Ruiz of the Federal Bureau of Investigation there exists reasonable grounds to believe that the subscriber information and cell site information requested will be relevant and material to an ongoing criminal investigation. The facts supporting this conclusion include the following:

On April 6, 2011, officers from the Detroit Police Department arrested four individuals believed to be involved in a series of armed robberies of Radio Shack and T-Mobile stores in Detroit, Michigan.

On April 26, 2011, a cooperating defendant was interviewed about his involvement in those armed robberies and admitted he had a role in nine different robberies that started in December of 2010 and lasted through March of 2011 at Radio Shack and T-Mobile stores in Michigan and Ohio. The defendant further admitted that others involved with the armed robberies were not taken into custody when he was arrested. The core members were usually the same three individuals, but they regularly brought in others to assist as getaway drivers and lookouts. The defendant identified 15 other individuals who had been involved in at least one of the nine robberies. Seven of those individuals had been involved in multiple armed robberies and three had been involved in at least five of the robberies. The defendant also stated that some of the individuals not in custody had been planning to rob more stores in Dayton, Ohio.

The cooperating defendant provided his cellular telephone number and identified numbers of some of the individuals involved. A review of the historical call detail records revealed other numbers that were contacted during and around the times of the robberies.

It is anticipated that the requested records will assist in identifying and locating the other individuals believed to be involved in the armed robberies.

Additionally, the requested telecommunications records should yield information that is relevant and material to corroborate surveillance information and may identify potential witnesses and/or targets. The requested information will therefore further the Federal Bureau of Investigation in their investigation and provide evidence that Timothy Sanders, Timothy Carpenter and other known and unknown individuals are violating provisions of Title 18, United States Code; §1951.

Applicant requests that the Court issue an Order pursuant to Title 18, United States Code, Section 2703(d) directing the **telecommunication carriers** to provide the requested records to agents of the Federal Bureau of Investigation.

Applicant further requests that this application and Order be sealed by the Court until such time as the Court directs otherwise, since disclosure at this time would seriously jeopardize the investigation, and that the Court order the **telecommunication carriers** their agents and employees not to disclose the existence of this Order or of this investigation to the subscriber, or to any

other person unless otherwise directed by the Court.

Applicant further requests that this Court's Order apply not only to the telephone numbers listed above for the target telephone numbers, but also to any changed telephone number(s) subsequently assigned to an instrument bearing the same [ESN][IMSI][SIM][IMEI][MSID][MIN] as the target telephone numbers, or any changed [ESN][IMSI][SIM][IMEI][MSID][MIN] subsequently assigned to the same telephone numbers as the target telephone numbers, or any additional changed telephone number(s) and or [ESN] [IMSI] [SIM] [IMEI][MSID][MIN] listed to the same subscriber and/or wireless telephone accounts as the target telephone numbers within the period authorized by this Order.

WHEREFORE, it is respectfully requested that the Court grant an Order directing the **telecommunication carriers** to (1) provide the requested records to agents of the Federal Bureau of Investigation; (2) not to disclose the existence of this Order or the investigation to the subscriber or customer or to any unauthorized person unless or until ordered or authorized to do so by the court; and (3) sealing this application and accompanying Order.

Respectfully submitted,

Barbara L. McQuade
United States Attorney

John N. O'Brien
Assistant U.S. Attorney

Dated: Jun-7 2011

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER FOR DISCLOSURE OF TELECOMMUNICATIONS RECORDS
_____/

Tracking No.: 11US60044-C
Hon. Stephen J. Murphy, III

ORDER

This matter, having come before the court pursuant to an application under Title 18, United States Code, Section 2703(d) by John N. O'Brien, an attorney for the Government, requesting the production of certain telecommunications records; the court finds that the applicant has certified and demonstrated to the Court that there are reasonable grounds to believe that the information sought is relevant and material to a legitimate law enforcement investigation into possible violations of Title 18, United States Code, §1951.

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d), that

Adelphia Communications, Adelphia Long Distance, Airlink Wireless, Airvoice Wireless, Allegiance Telecom of California, Inc., AllTel Communications, Alltel Georgia Communications Corp, AllTel Telephone Services, American Cellular, American Paging, Ameritech Michigan, Arch Communications, Arch Paging Commun-

ications, Arch Wireless; Astound, AT&T Broadband, AT&T Local Service, AT&T Long Distance, AT&T Wireless Services, Bay Star Communications, Bell South Telecommunications, Bittell Communications, Bluegrass Cellular, Bullseye Telecom, Cavalier Business Communications, Comcast Cable Communications, CCT Telecom, Cellco Partnership doing business as Verizon Wireless, Cellnet Communications, Cellular Information Systems of Florence, Cellular One, Cellular South, CelluPage, Central Telephone Company of Nevada doing business as Sprint of Nevada, Central Wireless Partnership doing business as Sprint PCS, Cincinnati Bell, Cingular Wireless, Comm South Companies, Commonwealth Communications, Competitive Communications, Inc., Comstat Mobile, Corecomm Limited Cox Communications, Cox Communications Arizona, Dobson Cellular, Crickett Communications, Inc., Cue Paging, DBS Communications, Dobson Communications, Duo County Telephone, Easton Telecomm Service; Edge Wireless LLC, Electric Lightwave, Embarq, Encompass Communications, Ernest Communications, Evans Telephone Company, Excel Communications, Excel Telecommunications, Focal Communications Corporation, Frontier: A Citizens Communications Company, Genesis Communications International, Global Crossing, GTE Paging, Granite Telecommunications, Hartington Telecommunications, Highland Telephone Co-op, ICG Communications, ICG Telecom Group, Iridium North America, ITC Deltacom, IXC Communications, J.D. Services,

KMC Telecom, Leap Wireless, Level 3 Communications, Inc., Long Distance Management, Long Distance of Michigan, MCI-Worldcom, MCI- Worldcom Wireless, Metrocall, Metro PCS, M Power Communications, Nationwide Paging, Navigator Telecommunications LLC, Network Telephone, Networkservices L.L.C., NII Communications, Inc., NSC Communications, O1 Communications, OCI Communications, Omega Services, LLC, One Communications, One Star Long Distance, Optel Texas, Inc. Pac West Telecommunications Incorporated, Pacific Bell, Pactec, Page Plus Communications, Pagemart, Phonetec, Qwest Communications, RCN Communications, Revol, Roseville Telephone Company, Sage Telecom, SBC Ameritech, SBC California, SBCCommunications, SBC Nevada Bell, SBC Pacific Bell, SBC Southwestern Bell. Seren Innovations, SkyTel Nationwide, Source One Wireless, Southwestern Bell, Southwestern Bell Wireless, Sprint-Nextel Corporation, Sprint Communications, Sprint Long Distance, Sprint Spectrum L.P., TCG America, Inc., TDS Metrocom, Inc., Telenet Worldwide, Telepacific Communications, Telescape Communications, Teligent, Time-Warner Cable, Time-Warner Telecom, Tracfone Wireless, Inc., Transtel, Trinsic Communications, T-Mobile USA Inc., T-Mobile/Omnipoint, US Cellular, US TelePacific Corp doing business as TelePacific Communications, Variatee Wireless, Verizon California, Verizon District of Columbia, Verizon Maryland, Verizon New England, Verizon New Jersey, Verizon New York, Verizon Northwest,

Verizon Texas, Verizon Wireless, Verizon Wireless Paging, Weblink Wireless, Virgin Mobile, VoiceStream Wireless, West Coast PCS LLC doing business as Sure West Wireless, Western Wireless Corporation, Wide Open West, Winstar Communications, WorldCom, XO Communications, Xspedius Communications (hereinafter the **telecommunication carriers**)

disclose and furnish the Federal Bureau of Investigation the transactional records described below which pertain to the following telephone numbers, hereafter referred to as "target telephones":

(313) 412-6845
Metro PCS telephone number roaming on Sprint's cellular tower network

The transactional records requested include:

A. All subscriber information and toll records including listed and unlisted numbers dialed or otherwise transmitted to and from target telephone from March 1, 2011 to March 7, 2011.

B. Records, credit and billing records, can be reached numbers (CBR), custom calling features, and primary long distance carrier, and caller ID for the target telephones.

IT IS FURTHER ORDERED pursuant to 18 U.S.C. Section 2703(c)(l)(B) and 2703(d), that the wireless carriers shall provide the locations of cell/site sector (physical addresses) for the target telephones at call origination and at call termination for incoming and outgoing calls during the relevant time period.

IT IS FURTHER ORDERED that this application and Order be sealed by the Court until such time as the Court directs otherwise, since disclosure at this time would seriously jeopardize the investigation; and the Court orders that the telecommunication carriers their agents and employees not to disclose the existence of this Order or of this investigation to the subscriber, or to any other person unless otherwise directed by the Court.

IT IS FURTHER ORDERED that this authorization applies not only to the telephone numbers listed above for the target telephone numbers, but also to any changed telephone number(s) subsequently assigned to an instrument bearing the same [ESN][IMSI][SIM][IMEI][MSID][MIN] as the target telephone numbers, or any changed [ESN][IMSI][SIM][IMEI][MSID][MIN] subsequently assigned to the same telephone numbers as the target telephone numbers, or any additional changed telephone number(s) and or [ESN][IMSI][SIM][IMEI][MSID][MIN] listed to the same subscriber and/or wireless telephone account as the target telephone numbers within the period authorized by this Order;

IT IS FURTHER ORDERED that the local, long distance and wireless carriers be compensated by the investigative agency for reasonable expenses incurred in providing technical assistance.

A True Copy
U. S. Attorney's Office
Eastern District of Michigan
By _____
Foreign Specialist

Honorable Mark A. Randon
United States Magistrate Judge

Dated: 6/7/11

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Cellular Analysis

(313) 579-8507
(313) 412-6845

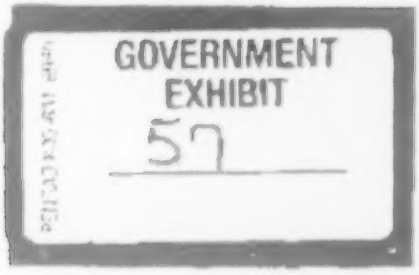
SA Christopher J. Hess

Detroit Division

Detroit Major Crimes Task Force

281R-DE-105923

November 5, 2013



INVESTIGATIVE INFORMATION

CASE FACTS: Special Agent Vicente Ruiz, Federal Bureau of Investigation, Detroit Division, investigated a case involving multiple armed robberies dating back to 2010. The robberies occurred in the Detroit metropolitan area as well as Warren, Ohio. Investigators linked cellular telephone number (313) 579-8507 to Timothy Sanders (Target Cell Phone 1) and (313) 412-6845 to Timothy Carpenter (Target Telephone 2).

REQUESTING INFORMATION

PURPOSE OF ANALYSIS: SA Ruiz requested cell site analysis of the target phones to determine the geographic area where the target phones were located in relation to incident date(s) and time(s).

TARGET CELL PHONE 1 INFORMATION

SERVICE PROVIDER: T-Mobile

SUBSCRIBER INFORMATION: N/A

TYPE OF RECORDS BEING ANALYZED: Call Detail Records (CDRs)

SOURCE FROM WHICH RECORDS ACQUIRED: SA Vicente Ruiz furnished an electronic copy of records associated with Target Phone 1.

DATE & TIME RANGE USED FOR ANAYLSIS:

03/04/2011, 2:52 p.m.

TARGET CELL PHONE 2 INFORMATION

SERVICE PROVIDER: Metro PCS

SUBSCRIBER INFORMATION: Michael Mayers

TYPE OF RECORDS BEING ANALYZED: Call Detail Records (CDRs)

SOURCE FROM WHICH RECORDS ACQUIRED: SA Vicente Ruiz furnished an electronic copy of records associated with Target Phone 2.

DATE & TIME RANGE USED FOR ANAYLSIS:

12/13/2010, 10:35 a.m.

12/18/2010, 4:50 p.m.

03/04/2011, 2:52 p.m.

04/05/2011, 2:40 p.m.

BASIC PRINCIPALS UTILIZED IN RECORD ANALYSIS

TECHNOLOGY

Cell phones are RADIOS that use RADIO FREQUENCIES to communicate. Some additional facts:

- Cell phones (when "on") constantly scan their environment looking for the best signal from the tower.

- The best signal generally comes from the

tower that is CLOSEST to the phone, or in its direct LINE OF SIGHT.

- The tower with the best signal is the one the handset will use for service, this is the serving cell and will be used to make and receive calls

- The phone will use the serving cell to make/receive calls.

- The phone "sees" other towers around the SERVING CELL and will constantly measure those signal strengths. However the phone will not randomly reselect to an adjacent tower unless the tower is on its "neighbor list" which is controlled by the network service provider. This allows the network to accurately manage and control the subscribers.

- As the phone moves, it will choose a new serving cell based on signal strength and neighbor list. If this occurs while the phone is in a call, the phone will "handoff" the call to the next cell site/sector. Therefore some service providers, such as SPRINT and AT&T, show a "beginning cell site" (call originated) and an "ending cell site" (call ended) in their records.

CELL SITES AND SECTORS

Cell towers (also known as CELL SITES or BASE TRANSCEIVER STATIONS) come in all shapes and sizes and can be located anywhere (church steeples, water towers, sides of buildings, etc.).

- A typical cell tower has THREE, 120° sectors. The service provider sometimes labels the sectors numerically, such as 1, 2, 3, or ALPHA, BETA, GAMMA. Sector 1 (or Alpha) typically covers the NORTHERN sector of the tower, 2 (EAST), 3 (WEST).

- It is important to note that each BTS has its own unique identifier, this identifier is used to track which towers the handsets use and is like a fingerprint on the network. It is not duplicated anywhere else.

- The location of a cell tower is often determined by sales/ marketing, capacity, improvement of coverage, or expansion/growth of a service provider. Generally there are more towers with overlapping coverage in urban areas; less towers (less coverage) in rural areas.

- Antennas on cell towers have downward tilt and are pointed towards the earth. The antenna arrays are fine tuned to provide a specific area of coverage. As RF travels away from the tower, their strength (and distance) diminishes. A good illustration of this principle is to think of a cell tower and the area that it covers as an upside down funnel.

Cellular Phone Record Analysis of (313) 579-8507

Date Range: 03/04/2011, 2:52 p.m.

ANALYSI S (313) 579-8507 (Target Telephone 1)

A review of the Call Detail Records (CDRs) revealed that there was call activity during the period covered by the records. The analysis was focused on the specific date and time referenced above. The CDRs contained the cell sites associated with each call event. The cell sites identified on the call detail records were compared to T-Mobile tower records. The tower records were imported to Microsoft MapPoint to visually depict the locations of towers within the T-Mobile network in the Detroit and Ohio markets. The cell sites identified on the CDRs were then plotted utilizing the corresponding tower records.

As a result, during the specified date, cell sites that were utilized by Target Telephone 1 were concentrated within the Warren, Ohio area. Analysis of the specified time period yielded the following results:

> 03/04/ 2011: A call was initiated at 2:20 PM. The duration of the call activity was over 31 minutes. The call originated and terminated on cell site 8499 5703 located in the geographic area consistent with the robbery scene at 2553 Parkman, Warren, Ohio.

A representation of this analysis can be seen in the attached Microsoft PowerPoint presentation labeled Attachment A.

Cellular Phone Record Analysis of (313) 412-6845

Date Range: 12/13/2010, 10:35 a.m.; 12/18/2010, 4:50 p.m.; 03/04/2011, 2:52 p.m.; 04/05/ 2011, 2:40 p.m.

ANALYSIS (313) 412-6845 (Target Telephone 2)

A review of the Call Detail Records (CDRs) revealed that there was call activity during the period covered by the records. The analysis was focused on the specific dates and times referenced above. The CDRs contained the cell sites associated with each call event. The cell sites identified on the call detail records were compared to the tower records furnished by Metro PCS. The tower records were imported to Microsoft MapPoint to visually depict the locations of towers within the Metro PCS network in the Detroit Metropolitan Area. On 03/04/2011, Target Telephone 2 was located outside of the Metro PCS market and roaming on the Sprint PCS network in Ohio. Sprint PCS tower records in the Ohio market were imported to Microsoft MapPoint as well. The cell sites identified on the CDRs were then plotted utilizing the corresponding tower records.

As a result, cell sites that were utilized by Target Telephone 2 were in the Detroit, Michigan and Warren, Ohio. On Analysis of the specified time periods yielded the following results:

> 12/13/2010, 10:35 a.m.: Call activity immediately prior to the reported time of the robbery utilized tower 127, sector 1 and sector 2. The tower is located

southwest of the robbery scene. The next call originated on an adjacent tower north of the robbery scene.

12/18/2010, 4:50 p.m.: Call activity in and around the time of the robbery incident utilized tower 173 and tower 188. The towers are located south of the robbery scene.

03/04/2011, 2:52 p.m.: Call activity before and after the robbery utilized tower 208 293 on the Sprint network. The tower is located south of the robbery location.

04/05/2011, 2:40 p.m.: Call activity prior to the robbery incident utilized tower 502 and tower 170. Tower 502 is located south of the robbery scene.

A representation of this analysis can be seen in the attached Microsoft PowerPoint presentation labeled Attachment B.

CONCLUSION

LOCATION OF TARGET CELL PHONE: Based upon my training, experience, and analysis, it is determined that:

Target Telephone 1 utilized cell sites in the geographic area consistent with the robbery scene located at 2553 Parkman, Warren, Ohio on March 4, 2011.

Target Telephone 2 utilized cell sites in the geographic area consistent with the robbery scenes on December 13 and 18, 2010, as well as March 4, 2011, and April 5, 2011.

ATTACHMENT A

Target Number (313) 579-8507

March 4, 2011, 2:52 p.m.

- Call activity was initiated at 14:20 (2:20 p.m.) lasting over 31 minutes.
- The activity originated and terminated on cell site 8496 5703.

ATTACHMENT B

Target Number (313) 412-6845
December 13, 2010, 10:35 a.m.

Target Number (313) 412-6845
December 18, 2010, 4:50 p.m.

Target Number (313) 412-6845
March 4, 2011, 2:52 p.m.
Metro PCS
Sprint PCS

Target Number (313) 412-6845

April 5, 2011, 2:40 p.m.